Guidelines For Classification And Construction

Part 4 Special Equipment and Systems

Volume 4

GUIDELINES FOR MARITIME CYBERSECURITY

2021

Biro Klasifikasi Indonesia

www.bki.co.id

Guidelines For Classification And Construction

Part 4 Special Equipment and Systems

Volume 4

GUIDELINES FOR MARITIME CYBERSECURITY

2021

Biro Klasifikasi Indonesia

Jl. Yos Sudarso No. 38-40, Tanjung Priok
Jakarta 14320 - Indonesia
rules@bki.co.id
www.bki.co.id

The following Guidelines come into force on 1st March 2022.

Foreword

This Guidelines for Maritime Cybersecurity is a new Guidelines which developed to provide the framework for implementation of cybersecurity on cyber-enabled equipment and/or cyber-enabled system on ships, offshore structures, and shore facilities.

Three Cybersecurity levels, Informed, Advanced and Adaptive are provided. These levels describe the level of cybersecurity capabilities in the company. Additional cybersecurity notations (CS-1, CS-2, CS-3) will be assigned to the ships and offshore structures that comply with the requirements of this Guidelines. The Cybersecurity Ship Certificate (CSC) will be awarded to the operating Company of the ship and offshore structures with CS notations upon achieving compliance to the corresponding Cybersecurity level in this Guidelines. The Cybersecurity Certificate (CC) may be given to the company who requested to certify their shore facility and found to comply with this Guidelines.

This Guidelines consist of 5 Sections, namely:

Section 1, General

Section 2, Cyber security development program

Section 3, Cyber security management system

Section 4, Requirements for Cybersecurity System

Section 5, Survey and Maintenance of Class

The electronic version of this Rules is available at BKI website, www.bki.co.id. Once downloaded, the Rules will be an uncontrolled copy. Please check the website for the valid version.

Further quires or comments concerning to the Rules are welcomed through communication to BKI Head Office.

This page intentionally left blank

Table of Contents

This page is intentionally left blank

Section 1 General

A. General

1. General Requirements

These Guidelines is developed to provide the requirements for evaluating and managing the Cyber risk of Ships and offshore structures as well as their operating companies. An additional class notation will be given to ships and offshore structures (fixed offshore structure or floating offshore structure) which comply with the requirements specified in this Guidelines as indicated in D. When requested, BKI can also assess, verify, and certify the associated shore-based facilities, as specified in the Section 4.

These guidelines present a framework to implement the Cyber safety programme on board a ship, offshore structures, and corresponding shore-based facilities. The requirements in these Guidelines will be used by BKI in the cybersecurity reviews and surveys of information technology (IT) systems; operational technology (OT) control systems; and their system interfaces and software on ships, offshore structures and associated shore-based facilities.

2. Scope and application

2.1 Scope

The requirements in this Guidelines are applicable to the computer-based information technology and operational technology systems that may be installed on board of ship, offshore structures, or shore-based Company facilities.

The application of cybersecurity program is generally categorized into the following categories:

- **New Construction**. New development of a cybersecurity program with a new construction (ship, offshore or interfacing facility) in accordance with the owning Company's security and other guidelines and requirements.
- **New System.** Development of cybersecurity for a new system, application or appliance, to be incorporated or integrated into ship or offshore security program with either an existing or a new security program in effect.
- **Existing construction.** Existing System of system (ship, offshore platform, or other maritime facility with multiple existing standalone and networked systems) upon which a security program must be overlaid in accordance with company security and governance needs.
- **Existing System.** Existing System for functional contribution to an existing construction, new construction, or an interfacing facility, which may be networked or standalone.

The cybersecurity requirements consist of three level of requirements. Those levels describe the boundaries of critical systems in the shipboard networked environment.

Primary Essential Services, as defined by system categories and criticality to human, asset or environmental safety, are to be protected for a ship or unit, within the defined system boundaries. For the definition of Primary Essential Services refer to Rules for Electrical Installations (Pt.1, Vol.IV) Sec.1.B Table 1.1 or Rules for Electrical Installations (Pt.5, Vol.V) Sec.1, B.2.2 and particular Rules in Part 5 Offshore Technology.

2.2 Application

These Guidelines are intended for use by the company operating all types of ships and offshore structures. The requirements set out in these Guidelines are stated in general terms to apply to various ships type and offshore structures as well as their operating Companies.

A vessel or offshore structures may be certified without certifying its operating Company or its facilities and vice versa so long as appropriate boundaries are defined and verified in accordance with these Guidelines.

B. Definition

The following definitions in Table 1.1 are used in this Guidelines.

Table 1.1 Definitions

Item	Descriptions
Acceptable Risk	Risk that can be tolerated by the Company having regard to its legal obligations and its own OH&S policy.
Administration	The Government of the State whose flag the ship is entitled to fly.
Anniversary Date	The day and month of each year that corresponds to the date of expiry of the relevant document or certificate.
Audit	Systematic, independent, and documented process for obtaining “audit evidence” and evaluating it objectively to determine the extent to which “audit criteria” are fulfilled.
Auditor	Person with the competence to conduct an audit.
Boundaries	Physical or site limits and/or organizational limits defined by the Company. (ISO50001:2011)
Capability	The ability to execute a specified course of action.
Company	The Owner of the ship or any other organization or person, such as the manager or the bareboat charterer, who has assumed the responsibility for operation of the ship from the ship owner and who, on assuming such responsibility, has agreed to take over all duties and responsibilities imposed by the ISM Code and this Guidelines; Organization [ISO 9001:2015, ISO 14001:2015, ISO 50001:2011, and OHSAS 18001:2007]. For Government-owned vessels in non-commercial service, the Naval Administration is to be considered the Company.
Company Information Security Officer (CISO)	The individual responsible for information systems, control systems and data security within the Company’s enterprise
Compliance	Confirmation decision by BKI that the Company and/or ship management system meets the applicable requirements of this Guidelines.
Continual Improvement	Recurring process of enhancing the management system in order to achieve improvements in overall performance.
Control System	Set of devices that manages, commands, directs or regulates the behavior of other devices or systems according to user inputs, settings or configurations.
Correction	Action to eliminate a detected non-conformity.
Corrective Action	Action to eliminate the cause of a detected nonconformity or other undesirable situation.
Cyber-Enabled System	Computerized or programmable system built to provide significant degrees of automation in operational function, system monitoring and management, or data communications.

Table 1.1 Definitions (*continued*)

Item	Descriptions
Cybersecurity Management System	An organizational tool for the identification, prioritization, execution and monitoring of the Company’s cybersecurity policies, processes and procedures
Demilitarized zone (DMZ)	Physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet.
Information Security	is the security applied to information (rather than systems) protecting it from unauthorized access, disclosure, modification or destruction.
Information Technology (IT)	The application of science to the processing of data according to programmed instructions in order to derive results. In the widest sense, IT includes all information and all technology; in a much narrower sense, telecommunications technology is excluded - or for some particular reason needs to be emphasized.
Intrusion Detection System (IDS)	is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports. Intrusion detection systems (IDS) provide real-time monitoring of network traffic. An IDS can detect a wide range of hostile attack signatures (patterns), generate alarms to alert operations staff and, in some cases, cause routers to terminate communications from hostile sources.
Intrusion Prevention Systems (IPSs)	also known as Intrusion Detection and Prevention Systems (IDPSs), are network security appliances that monitor network and/ or system activities for malicious activity.
Malware	Software designed to infiltrate or damage a computer system without the owner's informed consent
Operational Technology (OT)	A hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. It includes devices, sensors, software and associated networking that monitor and control onboard systems.
Organization	Organization means ship owner/ manager /bare boat charterer of ship / offshore installation (For the purpose of these Guidelines).
Penetration Testing	A penetration test, commonly referred as ‘pen test’, is an authorized simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system's features and data.
Phishing	A technique used to trick computer users into revealing personal or financial information. A common online phishing scam starts with an e-mail message that appears to come from a trusted source but actually directs recipients to provide information to a fraudulent Web site.
Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid. Some forms of ransomware encrypt files on the system's hard drive (a.k.a. crypto-viral extortion), while some may simply lock the system and display messages intended to coax the user into paying.
Recovery Planning	The development and implementation of plans, processes, and procedures for recovery and full restoration in a timely manner, of any capabilities or services that are impaired due to a cyber-event.
Router	A device that sends, or routes, information between two networks (for example, between a home network and the Internet).
Social Engineering	The practice of penetrating system security by tricking individuals into divulging passwords and information about network vulnerabilities. Often done by calling the individual on phone and pretending to be another employee of company with a computer-related question.
Spyware	A program that collects information, such as the web sites a user visits, without adequate consent. Installation may be without prominent notice or without the user's knowledge.
Virtual Local Area Network VLAN	A logical grouping of hosts on one or more local area networks (LANs) that allows communication to occur between hosts as if they were on the same physical LAN.
Virus	Virus is a hidden, self-replicating section of computer software that maliciously infects and manipulates the operation of a computer program or system.
Worm	Self-propagating malicious code that can automatically distribute itself from one computer to another through network connections. A worm can take harmful action, such

Table 1.1 Definitions (*continued*)

Item	Descriptions
Worm (*continued*)	as consuming network or local system resources, possibly causing a denial-of-service attack.

C. Condition of Certification

1. General

1.1 As a condition of certification, Companies applying for Certification according to this Guidelines are to conform to the requirements of the ISM Code as relevant to the selected scope of their organizational management system.

1.2 The company is to define the scope of certification which may include the ship, offshore structures, and/or the Company's facilities in combination(s) chosen by the Company. Ship selection considers all ship in the fleet but centres on the ship considered highest priority by the Company. At least one vessel of each selected type is to be presented as a sample to be maintained within the same scope of certification as required by the Company. The Company is to provide evidence of verifiable similarity[1] among ships and offshore structures of specific types if any survey or test operations are to be abbreviated on the basis of identical installations or commonality across ships and offshore structures.

1.3 Ships and offshore structures assessed to the requirements of this Guidelines are, as a prerequisite, to be Classed by BKI or Transfer of Class from other Classification Society members of International Association of Classification Societies (IACS) to confirm this Guidelines requirement are applied to existing safe, monitored and managed assets. In the case of critical equipment or systems requested for specific review under the terms of this Guidelines, those systems must be Classed by BKI or IACS member prior to consideration, for the same reasons as for ships and offshore structures Class requirements.

1.4 BKI registered ships or offshore structures found to meet the requirements with specified in this Guidelines will be assigned with Notation **CS-1**, **CS-2** or **CS-3** corresponding to their cybersecurity level (Informed, Advanced or Adaptive, respectively). BKI may also issue a "Statement of Fact" to ships and offshore structures which are not intended to be assigned with Cybersecurity Notation provided that they are conform with the requirements of this Guidelines.

The ship or offshore structure with Cybersecurity Notation (**CS-1**, **CS-2** or **CS-3**) or complying the requirements in this Guidelines corresponding to the cybersecurity level, will be issued Cybersecurity Ship Certificate (CSC) as requested.

As requested, a Company whose facility is assessed by BKI and found to meet the requirements specified in this Guidelines corresponding to cybersecurity level, may be issued a Cybersecurity Certificate (CC).

Table 1.2 summarize the application of condition of certification.

The cybersecurity levels are specified in D.

Table 1.2 Matrix of application

Object	Notations (CS-1, CS-2, CS-3)	CC	CSC	Statement of fact
Shore facilities		X		

[1] Similarity includes not just type design (unit 1, unit 2, of a series), but also similarity of control system construction and implementation. Programmable Logic Controllers (PLCs) used in specific systems must be shown as sufficiently similar across units with a ship type that understanding of control systems is possible through documentation of those systems.

Table 1.2 Matrix of application (*continued*)

Object	Notations (CS-1, CS-2, CS-3)	CC	CSC	Statement of fact
Management systems (ship/offshore)			X[1]	X[3]
Ship or offshore BKI classed	X		X[2]	X[3]
Ship or offshore non-BKI classed				X

[1] Including information of cybersecurity level applied by the company (informed, advance, adaptive)

[2] If the ship is found to comply with the **CS** notations, the **CSC** will be given to the operating company.

[3] The statement of fact and/or assessment report may be issued by **BKI** upon requested by owner.

1.5 Ship shall be Surveyed on an annual basis, when there are major cyber-enabled, safety-related networked system configuration changes[2], or with multi-year Class survey events when no major system configurations are changed. Annual Surveys are to be performed within three months before or after each anniversary date of the crediting of the previous Special Periodical Survey or original construction date. Surveys/Audits for compliance to this Guidelines will be harmonized with extant BKI Classification and Statutory survey/audit cycles to the extent possible.

1.6 All certifications are non-transferable. Assessments are based upon a sampling process. The absence of recorded nonconformities does not mean that none exist. Nothing contained herein or in any SOC, notation, or report issued in connection with a certifications and/or notation is intended to relieve any designer, builder, owner, manufacturer, seller, supplier, repairer, operator, insurer, or other entity of any duty to inspect or any other duty or warranty, express or implied, nor to create any interest, right, claim, or benefit in any insurer or other third party.

1.7 This Guidelines is subject to change and revision. All Guidelines related modifications/amendments need to meet the latest version of the Guidelines and major changes may require the entire system be recertified to the latest version of the Guidelines. The survey requirements are to be conducted to the latest editions of the Guidelines.

BKI reserve the right to make any changes or updates retroactive.

2. Company responsibilities

The following responsibilities shall be fulfilled by companies who are looking for compliance to the requirements of this Guidelines. Some of which are more fully described in subsequent sections of the Guidelines:

1) Document, implement, and maintain a cybersecurity management system in accordance with the pertinent requirements of this Guidelines.
2) Provide BKI copies of Cybersecurity Management System documentation for review, in accordance with the requirements of this Guidelines.
3) Maintain a log or compiled record of all modifications, maintenance and system security or configuration updates and upgrades, including any outstanding help desk tickets or vendor/integrator repair or maintenance requirements, and any insecurities or breaches, and the resolution thereof (the log is to be in digital searchable format).
4) Allow BKI access to all certified locations and ships during appropriately scheduled working hours so as to assess the Cybersecurity Management System and relevant systems (information technology (IT), operational technology (OT), or both, including data infrastructure and interface systems) to determine continuing compliance with the pertinent requirements of this Guidelines.

[2] Examples of changes sufficient to force reassessment of cyber-enabled, safety-related networked systems include major-version-number operating system or firmware changes in either OT or IT; control system changeouts in safety-critical systems; or combined configuration changes between or among two or more systems that control safety-critical systems. Other examples also apply.

5) Notify BKI of port state detentions of vessel(s). In the case of cyber-enabled, safety-related system assessments, inspections or audits that result in unsatisfactory port state findings concerning systems included in the verification plan for this Notation, note to BKI the details of the same.

6) Inform BKI in writing when an ISM Document of Compliance (DOC) or Safety Management Certificate is withdrawn or invalidated by the issuing party for vessels certified to the requirements herein.

7) Submit plans and data as documented in Section 4.

8) Inform BKI in writing of major changes to organizational management system elements (e.g., managerial organizational structure, location, change in types of vessels operated, upgrade/downgrade of process capability, control, or flow) so that the changes may be evaluated by BKI and appropriate action taken.

9) Inform BKI when major modification related to the cyber-enabled, safety-related networked system (IT, OT, or both) takes place.

3. Capability Assessment Process

The assessment process requires development of a stage-wise risk profile for the ship, asset or facility.

An initial ship or asset assessment will be a multi-part event that may be conducted in one contiguous time period, if ship or asset personnel and documentation are available, or it may be broken into parts to better match Company needs. Each stage will encompass specific objectives and will deliver products particular to those objectives. The expected outcome of the entire process is a capability assessment that shows any remaining gaps or decisions required to satisfy the Company's cyber-enabled systems safety and security requirements, along with the appropriate certificate and/or Notation when the process is complete to BKI and Company satisfaction.

The overall assessment process is depicted in Fig. 1.1.

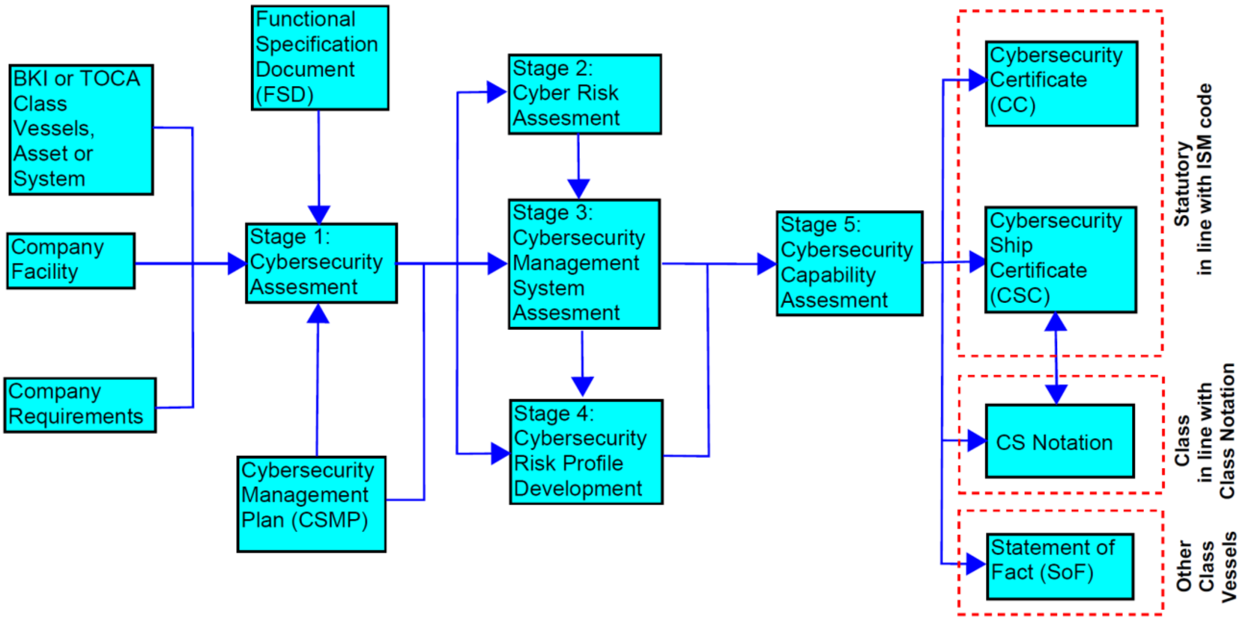
BKI or TOCA Class Vessels, Asset or System
Company Facility
Company Requirements
Functional Specification Document (FSD)
Stage 1: Cybersecurity Assesment
Cybersecurity Management Plan (CSMP)
Stage 2: Cyber Risk Assesment
Stage 3: Cybersecurity Management System Assesment
Stage 4: Cybersecurity Risk Profile Development
Stage 5: Cybersecurity Capability Assesment
Cybersecurity Certificate (CC)
Cybersecurity Ship Certificate (CSC)
CS Notation
Statement of Fact (SoF)
Statutory in line with ISM code
Class in line with Class Notation
Other Class Vessels

Fig. 1.1 Capability Assessment Process

3.1. Stage 1: Cybersecurity Assessment

The initial Cybersecurity Assessment includes asset enumeration, policies and procedures examination, architectural documentation examination, and asset comparison with the Functional Specification Document (FSD).

3.1.1 Functional Specification Document (FSD)

The FSD is the combined documentation associated with architecture, operations, security and testing of the mission-critical or business-critical systems aboard a ship, on an offshore asset, or in a facility. The expected content of an FSD is provided in 8 below.

3.1.2 Cybersecurity Management Plan (CSMP)

The CSMP is a mid-way stage to establish a Cybersecurity Management System (CSMS) if the Company does not have a method set in place to manage its critical systems' cybersecurity and safety postures. The CSMP is a work breakdown structure (WBS)-oriented program to develop and implement a capabilities-based Cybersecurity program.

3.2. Stage 2: Cybersecurity Risk Assessment (CRA)

Stage 2 includes asset risk condition assessment, with a functional protective measures comparison against Company requirements. Threat matching with the protective measures will reveal any gaps the Company may have. The stage provides an Initial Risk Profile at conclusion.

3.3. Stage 3: Cybersecurity Management System Assessment (CMSA)

Stage 3 assesses the Company's cybersecurity management across the organization and its assets, including automation methods, asset management and comparisons with the FSD, and cyber-related systems management and reporting. This stage provides templates and tools, as required.

3.4. Stage 4: Cybersecurity Risk Profile Development (CRPD)

Stage 4 compiles all management system, asset assessments and risk assessment outputs to develop the Company Risk Profile. This uses the risk progression developed through previous stages to provide a measurable achievement profile for continued progress toward capability set certification.

3.5. Stage 5: Cybersecurity Capability Assessment (CCA)

The CCA includes capability assessment, FSD assessment, interfacing systems assessment, networked systems audit, data integrity assessment and final certification for either CC or CSC and Notation.

4. Survey and Certification Process

4.1 Cybersecurity certification is an annual process for ships and/or offshore structures that seek to achieve and maintain the Notation and/or certificate. Survey for cybersecurity includes the factors listed in 2, emphasizing documentation, operational cybersecurity management system viability, strict control of configurations and changes in networked or cyber enabled assets, and organizational capabilities in place and functioning. Detailed checklists, supplementing the capability specifications in Section 5, will be provided for progress checking and current-status documentation.

4.2 Periodicity of survey for Cybersecurity Certification will harmonize with BKI Class Survey requirements, and BKI will coordinate surveys wherever possible.

4.2.1 Surveys During Construction, BKI Engineering and Survey personnel assigned to a newbuilding project will actively collaborate to check design such that safety principles are integrated, and that cybersecurity assessments and survey(s) are conducted in consonance with conventional survey events.

4.2.2 Surveys After Construction, the periodical survey process, including both Annual and Intermediate Surveys, will be supplemented by cybersecurity assessments as required. Annual Survey includes the documentation required in 2 above, given the fluid nature of information and automation technologies.

4.2.3 Occasional Surveys, cybersecurity surveys and assessments may be required after changes of equipment or control system (major system changes or configuration changes), after security events occurred, or on an as-required basis from the Company.

4.3 The certification will expire at the end of the stated period on the CC or CSC, normally 1 year. Reassessment, assuming documentation is provided (as in 2) and testing is completed in a timely fashion, is expected to be a shorter and more streamlined evolution than initial assessment.

4.4 Relationship between Survey and cybersecurity certification

Class, as maintained through regular Surveys, reviews overall technical and procedural compliance for requirements in accordance with the overarching Rules for Classification and Construction, outside the cybersecurity certification.

Class, especially in conditions of Continuous Survey, includes survey for Cybersecurity Notation when requested, though said survey is a snapshot in time within the Class continuum.

The BKI Class will be affected by the results of the cybersecurity certification only when/if safety-critical findings are found that are determined to compromise the safety of life, ship or asset, or the environment.

5. Representations

Notation and certification are a representation by BKI that at the time of assessment the Company and Ships, as pertinent, has established and implemented a Cybersecurity Management System in accordance with the requirements in this Guidelines, and that the assessments, inspections, and tests for appropriate security profiles and risk conditions were completed satisfactorily. Those Notation and certification are not a representation that the Company always acts in compliance with the cybersecurity program or that the cybersecurity program addresses all contingencies. Management performance remains the responsibility of the Company.

6. Termination

The continuance of certification or any notation is conditional upon the Company's and vessels' continued compliance with the pertinent requirements of this Guidelines. BKI reserves the right to reconsider, withhold, suspend, or cancel the assessment or Notation for noncompliance with the Notation requirements, refusing access to a vessel, unit, or facility for an assessment or verification, or non-payment of fees which are due on account of certification and other services.

Upon change of vessel or asset ownership, or of management organization, BKI reserves the right to perform out-of-cycle reassessments to check that the Notation remains current under the new organization. The essence of this Guidelines is building, maintaining and sustaining enabling capabilities for security and safety of cyber-enabled systems; a change in ownership or management will necessarily indicate a change in Company capability to support secure and effective operations in vessel or asset systems.

7. Limitation of Liability

BKI shall not be liable or responsible in any respect for any inaccuracy or omission in this Guidelines or any other publication or document issued by BKI related to this Guidelines. Every owner, builder, or operator must understand their systems in order to tailor the application of security controls and requirements, filling gaps in their security where needed by specific situations. This Guidelines is not meant to address every possible contingency, but rather provide a means by which owner/builder/operator may execute a security program that may, in operations, reveal needs for tailored or unique security controls.

8. Document to be Submitted

To support proper review in BKI assessments, the following documents are to be available to BKI for review. These documents comprise the Functional Specification Document (FSD) in a constructive form, and they provide the visibility and understanding required for system assessment.

Documents and named artifacts include many such as the following:

- Integrity level reviews
- Safety Instrumented Systems (SIS) functions and status
- Failure Mode, Effects and Criticality Analysis (FMECA) records and updates (upon major configuration changes)
- Test reports and documentation, with retests
- Data logs from control systems
- Operations and Maintenance (O&M) Plan
- Control Equipment Registry
- Software Registry
- Software Management of Change (SMoC) Plan, Policy and Process
- Software Change Management Plan (CM)
- Software Configuration Management Plan, Policy and Process

Other documents commonly contain valuable data supporting documented processes and operational test results. Documents containing the following data are also to be available:

- Conditional states
- Integrity levels of components/systems
- Production system interfaces
- Human-Machine Interface (HMI) instructions
- Software versions, firmware, hardware by spec
- Constraints on system operations, with reasons
- All other interfaces (non-HMI, Supervisory Control and Data Acquisition (SCADA), data collection, with protocols and constraints)
- System conflicts and unresolved software issues
- Hardware and software obsolescence plans
- Reliability, Availability, Maintainability and Supportability (RAM-S) reviews
- Safety reviews

D. Cybersecurity Level

1. The procedures and criteria given in this Guidelines are intended for cybersecurity implementation and subsequent verification for three levels of implementation.

2. Three different level of implementation is to define the safety level boundaries of specified safety related system in the ship or offshore structures. The non-safety related system as well as non-safety related function are not included in the level unless specified in the verification plan. The requirements for each cybersecurity level are increased from basic level to the adaptive level. The Cybersecurity level are as follows:

- **Cybersecurity Level 1:** Informed Cybersecurity

- **Cybersecurity Level 2:** Advanced Cybersecurity
- **Cybersecurity Level 3:** Adaptive Cybersecurity

3. The requirements for each cybersecurity level will be further described in Section 4. The brief comparison of the different cybersecurity level is showed in Table 1.2.

Table 1.2 Brief comparison of cybersecurity level

No.	Category	Informed	Advanced	Adaptive[1]
1	Asset Management	X	X	X
2	Governance	X	X	X
3	Risk Assessment	X	X	X
4	Physical & System access control	X	X	X
5	Network Security	X	X	X
6	System security controls	X	X	X
6.1	Data Security		X	X
6.2	Information Protection		X	X
7	Detection Procedures	X	X	X
7.1	Event monitoring		X	X
7.2	Cyber safety centre		X	X
8	Training, awareness & information sharing	X	X	X
9	Response and Recovery Procedures	X	X	X
9.1	Communication		X	X
9.2	Recovery management		X	X
10	Cyber Safety Process Review		X	X

[1] In principle Informed and Advanced requires similar category to be complied. However, for Adaptive additional requirements are assigned in each category in addition to requirement for Advanced as specified in Section 4.

E. Notation

1. Cybersecurity notation will be assigned upon achieving compliance corresponding to cybersecurity level.

The relation between cybersecurity levels and notations are as follows:

- **CS-1** complies with the requirement of **Cybersecurity Level 1:** Informed Cybersecurity
- **CS-2** complies with the requirement of **Cybersecurity Level 2:** Advanced Cybersecurity
- **CS-3** complies with the requirement of **Cybersecurity Level 3:** Adaptive Cybersecurity

Hierarchy of notations is depicted in Fig. 1.2

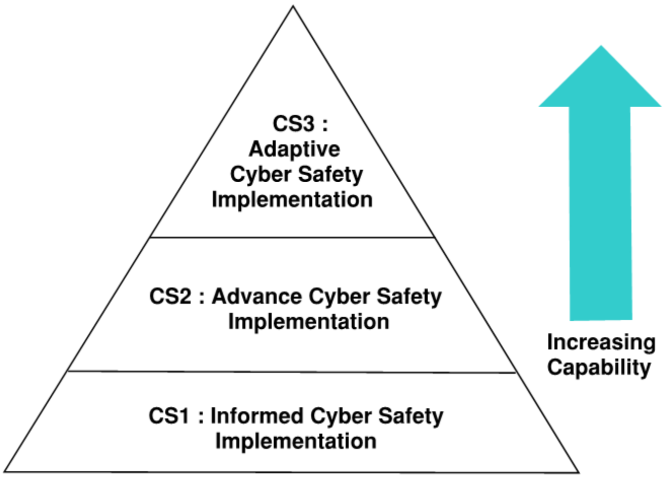
CS3 : Adaptive Cyber Safety Implementation
CS2 : Advance Cyber Safety Implementation
CS1 : Informed Cyber Safety Implementation
Increasing Capability

Fig. 1.2 Cybersecurity notation hierarchy

2. The **CS** notation will be given to the ship or offshore structures for the requested level of safety base on satisfactory completion of the Survey.

3. The maintenance of the cybersecurity notation by compliance of the Cybersecurity level over the operational life of the ships, offshore structures are subject to continued compliance and the satisfactory completion of periodic survey performed onboard of the ship, or at offshore structures.

F. Organization

1. Company

The Company is an organization that initiates the project and owns the information system and/or control system at the end of the project.

2. Ship Builder Integrator (SBI)

For new buildings, the SBI is the shipyard. If no shipyard is involved, then the activities and requirements associated with the SBI are to be performed by the Owner.

3. System Provider (SP)

System Providers (SP) are suppliers that developed the software for the system under software verification test subject to system verification. If multiple systems are selected for system verification, then there may be multiple SPs. This may also include Original Equipment Manufacturer (OEM) for majority of hardware systems.

4. Sub-Supplier (Component Providers)

A sub-supplier is a supplier of connected equipment to the SP’s control system and subject to integration portion of the verification testing.

G. Further rules and standards to be considered

1. BKI Rules

- Rules for Seagoing Ships (Part 1)
- Rules for Dynamic Positioning System (Pt.4, Vol.I)
- Guidelines for Autonomous Ships (Pt.3, Vol.1)

2. IEEE publications

- IEEE Std 14764-2006, Second edition 2006-09-01, Software Engineering – Software Life Cycle Processes – Maintenance
- IEEE Std 12207-2008, Second edition, 2008-02-01, Systems and software engineering – Software life cycle processes
- IEEE Std 730-2002, IEEE Standard for Software Quality Assurance Plans
- IEEE Std 1012-2004, IEEE Standard for Software Verification and Validation
- IEEE Std 1016-1998, IEEE Recommended Practice for Software Design Descriptions
- IEEE Std 1219-1998, IEEE Standard for Software Maintenance
- IEEE Std 1362-1998 (R2007), IEEE Guide for Information Technology – System Definition – Concept of Operations (ConOps) Document

3. IEC publication

- IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC 61511-1, Functional safety – Safety instrumented systems for the process industry sector
- IEC 62351 (Power systems management and associated information exchange - Data and communications security)
- ISA/IEC 62443 (Industrial Automation and Control Systems Security) Standard of Good Practice for Information Security (Published by the Information Security Forum (ISF))

4. ISO publication

- ISO 17894-2005 General principles for the development and use of programmable electronic systems in marine applications
- ISO/IEC 9126-1:2001 Software engineering – Product quality – Part 1: Quality model
- ISO 9001:2015, Quality Management Systems – Requirements
- ISO/IEC 20000-1:2011 Information Technology – Service Management - Part 1: Service management system requirements
- ISO/IEC 27001:2013 - Information Technology - Security techniques - Information security management systems – Requirements
- ISO/IEC 27002:2013 - - Information Technology - Security techniques - Code of practice for information security controls
- ISO 28001:2007 - Security management systems for the supply chain; Best practices for implementing supply chain security, assessments and plans - Requirements and guidance
- ISO 31000:2009 – Risk management – Principles and guidelines

5. IMO Regulations

- International Safety Management (ISM) Code as amended
- International Ship and Port Facility Security (ISPS) Code as amended

6. Other regulations/standards

- National Institute for Science and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity
- National Institute for Science and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations
- National Institute for Science and Technology (NIST) Special Publication 800-82 Guide to Industrial Control System (ICS) Security.
- IACS Recommendation 166, Recommendation on Cyber Resilience.

This page is intentionally left blank

Section 2 Cybersecurity Program Development

A. General

1. Cybersecurity is the application of security methods and controls to provide for, and to verify, deterministic behavior of cyber-enabled systems. A cybersecurity program is meant to safeguard assets, guide personnel and their actions, and allow freedom of action and of decision making within the boundaries of the system, free of interference from both internal and external influences. The cybersecurity process has a beginning but has no practical end short of decommissioning of the cyber-enabled asset.

Ship and offshore asset owners, operators and crew must understand their systems in order to use and protect systems, data, and asset functions. Poor cybersecurity can lead to loss of data or intellectual property; to loss of system integrity in both business-essential and business/mission/safety-critical systems; and to loss of system function in the critical control systems used to execute business processes. Cybersecurity can prevent losses when systems are designed, architected, engineered, built and operated with appropriate due care and due diligence.

2. Cybersecurity for systems must naturally provide security for people, data, systems and assets.

2.1 Security for people must include periodic awareness training, systems training, and security policies and procedures.

2.2 Security for assets includes the physical assets such as ships, offshore assets, associated shoreside facilities and equipment as well as the virtual assets such as business data, process information, and intellectual property.

2.3 An organization’s assets may also include its functions – operations which keep the Company to operate properly, and keep the processes to flow unhindered. Those functions that make the business viable are assets for the operation of the Company.

2.4 Operational technology (OT) or cyber-physical systems (CPS) will have relevance to safety in their environments because they control direct physical effects in connected systems. These OTs will often often communicate with information technology (IT) general-purpose networks to provide sensor or operational data to management personnel. Thus, cybersecurity for systems must consider both IT and OT aspect of the system and the possible connection between them which may have different trust levels, owners and operators.

B. Process

1. The Company is responsible for setting the cybersecurity policies for the systems and ships/offshore structures it operates. As a minimum those policies must conform to international and national requirements, but they will also reflect the Company’s objectives in maintaining safety and security onboard its ships wherever they operate. The elements of a cybersecurity program include the following as minimum elements:

- Company capabilities suitable for defense from cyber threats;
- Risk assessment of cyber threats;
- Management system scope and depth suitable for defense from cyber threats; and

– System and equipment design and engineering to minimize cyber vulnerabilities.

2. Requirements for Company

2.1 Five functional elements indicated by IMO guidelines on cyber risk management forms the basis of the requirements that shall be complied. These five elements are as follows:

- Identify (ID): defining key elements (personnel roles and responsibility, assets, data and capabilities) that pose risks to ship operations when disrupted
- Protect (PR): implementing risk control processes, measures and contingency plan to protect against cyber event
- Detect (DE): developing and implementing activities necessary to detect a cyber event in timely manner
- Respond (RS): developing and implementing activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event
- Recover (RC): Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event

2.2 The five functional elements are then expanded further as shown in Table 2.1. The detailed requirements derived from these items are explained in Section 4.

Table 2.1 Requirements expanded from IMO's five functional elements

Requirements	Element
1. Governance, Policies & Procedures	ID
2. Asset Management	ID
3. Risk Assessment	ID
4. Physical & System access control	PR
5. Network Security	PR
6. System security controls	PR
6.1 Data Security	PR
6.2 Information Protection	PR
7. Detection Procedures	DE
7.1 Event monitoring	DE
7.2 Detection procedures Cyber safety center	DE
8. Training, awareness & information sharing	PR
9. Response and Recovery Procedures	RS, RC
9.1 Communication	RS, RC
9.2 Recovery management	RC
10. Cyber Safety Process Review	RC
11. Asset Inventory	ID

3. Risk Assessment and Risk Management

A risk-based approach to cybersecurity requires the understanding of risk factors or risk conditions, with the business- or mission-based grasp of assets under risk. The implementation of this risk assessment and management depend on the cybersecurity level, see Section 5.E.4.

4. Management System

The Company's Cybersecurity Management System is to address cyber security concerns and be subject to audit. Section 3 defines the management system requirements for cybersecurity.

5. Systems and Equipment

5.1 Operational Technology (OT)

Increasing complexity of OT system must be understood, maintained, and tested quite differently than traditional IT networks and systems.

Connecting OT systems to conventional (non-engineering) networks for monitoring, remote access or convenience exposes the OT systems to outside connectivity, potentially revealing vulnerabilities that could affect cyber-physical system operations. Thus, the connection of OT to conventional networks needs to be managed.

The way forward relies on an understanding of the differences between OT-specific maritime cybersecurity and IT practices and appropriate handling. Policies and procedures must comprehend the differences in managing an OT network or system vs traditional IT methods.

5.2 System Categories

The judgment as to system category for safety-critical or safety-relevant systems will be considered in BKI Cybersecurity assessments. Systems with direct safety impact within their systems, or secondary systems that could bring about potential failures in safety-critical systems, will be considered as belonging to higher category than others that do not possess such features or functions. Sytem category is in accordance with Rules for Electrical Installations (Pt.1, Vol.IV) Sec. 10 and is represented as follows:

Table 2.2 System categories

Category	Effects	Typical system functionality
I	Those systems, failure of which will not lead to dangerous situations for human safety, safety of the ships or offshore structure and/or threat to the environment.	- Monitoring function for informational/ administrative tasks
II	Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the ships or offshore structure and/or threat to the environment.	- Alarm and monitoring functions - Control functions which are necessary to maintain the ship in its normal operational and habitable conditions
III	Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the ships or offshore structure and/or threat to the environment.	- Control functions for maintaining the ship's propulsion and steering - Ship safety functions

5.3 Security for All Components

Cybersecurity is generally focused on securing networks and devices on those networks. But other components must be included for defensibility and correct operations also. Transmission systems and lines must be safeguarded, whether by the Company or through its contracts with providers. Personnel must be trained for cyber-enabled system safety, resistance to criminal attack methods, and protection of organizational assets and critical systems or functions.

Resilience of critical systems is part of the cybersecurity implementation process. The result of resilience is that attacks or failures do not persist after incident response controls are executed and system restoration begun.

Defense in depth, the use of multiple means to view, protect and monitor networked assets, is an important part of resilience, as are architected solutions for designed-in resistance to unauthorized access or use; backup capabilities, such as redundant power or communications; user process definition as means to minimize errors or incorrect use; and system data restoration. Component security, with such features, helps confirm secure operational characteristics and integration with other systems in ways that do not introduce unexpected risks to the other systems. All these factors derive from the process and technology specifications in the Guidelines, combined with owner or operator insights or the assets protected.

5.4 Security and Remote Accessibility

Connections, communications and access to Internet Protocol (IP)-enabled sensors and systems that are considered components of the Internet of Things (IoT) or Industrial Internet of Things (IIoT) must be specifically addressed as part of the Operational Technology security measures onboard any ship, asset or facility. Remote accessibility to IoT/IIoT devices, especially, must be controlled carefully, as these devices are expected to be standalone, sealed, never-updated network participants, meaning that they can become conduits into primary networks if left exposed to unauthorized communications. These devices and similar systems are addressed in the OT specification in Section 4, with specific coverage under **Cybersecurity Level 2 – Advanced Cybersecurity**.

Cloud storage and application providers also fall into the category for remote access. Authorized procedures for application and storage access must govern all communications with these offboard resources. Because of the nature of cloud communications, the primary protective requirements are human procedures and processes (such use of access control lists match against asset usage), with technical controls that specifically identify the user (two-factor or multi-factor authentication) when in contact with sensitive information systems or assets.

5.5 Management of Change for All Components

Cybersecurity levels are dependent on owner/operator exercise of the capabilities as provided in the Guidelines, in addition to those capabilities and needs required by due diligence responsibilities, including management of change. When a ship or asset is certified according to this Guidelines, BKI is to be notified when major changes are made to configurations or systems; when new interfaces between IT and OT are implemented, or existing interfaces are changed; or when new remote access methods are implemented for either IT or OT. BKI will communicate with the ship or asset management/owner, and with both IT and OT points of contact in these matters to confirm complete communications and understanding of changes and configurations.

Section 3 Cybersecurity Management System

A. Management of Cybersecurity

A Company planning to build or develop its cybersecurity program for certification under BKI is to implement and monitor its security strategy and plan through a Cybersecurity Ship Management (CSM), which is the capability management and tracking management framework designated for use in cross-security practices, programs and processes. The CMS provides the management system nucleus for growing company capabilities to desired maturity levels; supporting operational understanding of security posture(s); satisfying audit requirements; and provisioning and maintaining Cybersecurity Continuous Monitoring (CCM) needs.

Company Security personnel implement the CSM as the direct flow-down from the overarching enterprise technology and security strategies and any related implementation plans. The CSM provides prioritization and management of efforts to mature and complete the security architecture and the organizational capabilities required to meet enterprise security needs. It is to be demonstrated that the CSM objectives:

1) Maintain capabilities in the Company to understand and manage
   - A) Systems and applications within the enterprise
   - B) Data repositories and data stores serving enterprise applications and uses
   - C) Data flows that support mission-critical applications
   - D) Data flows that support mission performance measures
   - E) Application performance measures and their indications applicable to security conditions
   - F) Relationships among individual system security postures
   - G) Overall networked system risk posture
2) Develop, maintain and sustain an integrated risk profile for the enterprise
   - A) Provide understanding of risk factors and possible risk impacts of threats, both external and internal, on overall mission, systems, data, organization, and facilities
   - B) Prioritize risk mitigation and issue remediation work efforts based on threats, vulnerabilities and exposures of vulnerable systems or features to threats
   - C) Certify system, unit, facility or organizational performance, and the ability to employ systems of systems for mission requirements
   - D) Provide incident response capability for mission resilience in the expected threat environment, in consonance with risk postures
3) Define sufficiency of protective measures and controls
   - A) All perimeter and monitoring devices communicate with the enterprise log management or Cybersecurity Information and Event Management (CIEM) system
   - B) All security, perimeter and monitoring systems provide dashboard displays to support Cybersecurity Continuous Monitoring (CCM)
   - C) All communication paths go through security systems for monitoring and traffic filtering
   - D) All web-based applications have web application protections (i.e., firewalling) in place
   - E) All enterprise systems have host-based protections that report through monitoring dashboards

- F) All security personnel understand monitoring measures and metrics, with ongoing training for continuity
- G) All workstations and data stores have backups in protected, segregated storage
- H) All enterprise personnel records and entities are part of the enterprise identity and access management regime;
- I) All software is tested throughout its lifecycle for security integration
- J) All enterprise systems are included in configuration, vulnerability and patch management processes
- K) Configuration, vulnerability and patch management processes are informed by threat research and intelligence to provide prioritization feedback to risk management authorities
- L) All enterprise systems are initially configured with, and managed through, system hardening guides in accordance with enterprise baseline and architectural controls
- M) Enterprise systems are included in a security systems manual book

4) Provide an integrated, interoperable security and perimeter device environment to enable
   - A) System automation, where advisable
   - B) Accelerated situational awareness and status understanding
   - C) Reduced staff requirements in data gathering
   - D) Shorter timelines for incident response, brought by quicker awareness
   - E) Improved daily system management, with greater supportability, reliability and maintainability

The CSM is the operational security management and reporting method which encourages completeness of effort, wholeness of security, and maturity of processes within the Company. Execution of CSM is to be applied across the entire Company. Proactive policies and protective controls are to be applied across the enterprise, modified to accommodate:

1) Physical locations for data and systems
   - A) Data centres and disaster recovery facilities
   - B) Physical facilities and document stores
   - C) Distributed digital data stores within facilities
   - D) Geo-limited data siloes with limited external accessibility
   - E) Endpoints and removable media
   - F) Physical storage locations for media and data
   - G) Mobile devices and storage
2) Logical locations for data
   - A) Endpoints
   - B) Mobile devices
   - C) Shared drives
   - D) Segregated storage drives
   - E) Collaborative data stores
     - a) Line of business data stores
     - b) Collaborative environment data stores (e.g., SharePoint)
   - F) Backup data sets
   - G) Cloud services: applications (software as a service)
   - H) Cloud services: storage (infrastructure as a service)

    I) Data archives

3) Access rules for data and enterprise functions, as classified as
    A) Roles
        a) Employees
        b) Contractors (on-site)
        c) Consultants (on-site)
        d) Contractors or consultants (off-site)
        e) Retired employees
        f) Customers
    B) Rules
        a) Project authorizations
        b) Need-to-know
        c) Minimum privilege
        d) Separation of duties
    C) Exceptions and special cases
        a) Service accounts
        b) Test accounts
        c) Developer accounts, especially when geographically remote.

CSM management is per the cybersecurity level implementation plan. Capabilities are tracked and reported as necessary inside the Company.

1. Cybersecurity Environment Aspects

The Company is to establish, implement, and maintain procedure to identify the contextual aspects of its shipboard and shore-based operations within the scope of the cybersecurity ship management that it can control and those it can influence, taking into account planned or new developments or new or modified activities and services. The Company is to determine which aspects of its current circumstance have or can have a significant impact on the cybersecurity conditions in the Company. The Company is to document this information and keep it up-to-date in the Risk Management Plan and/or in the cybersecurity Functional Specification Document (FSD).

The Company is to take into account the significant contextual aspects when establishing, implementing, and maintaining its cybersecurity management system.

2. Cybersecurity Implementation Planning

The Company is to conduct and document a cybersecurity planning process. Cybersecurity planning shall be consistent with the Company's technology Acceptable Use Policy and shall lead to activities that continually improve performance. Cybersecurity planning is to involve a review of the Company's activities that can affect relative risk management performance.

3. Cybersecurity Hazard Identification, Risk Assessment, and Risk Control

3.1 Procedures

The Company is to establish and maintain procedures for the ongoing cyber-physical system hazard identification, risk assessment, and determination of necessary controls. The procedure for cyber-physical system or process hazard identification and risk assessment is to take into account:

1) Routine and non-routine activities involving the systems;
2) Activities of all personnel having access to the workplace (employees, contractors, consultants, and including subcontractors, third party suppliers and visitors);
3) Human behaviour, capabilities, and other human factors in usability and potential effects of cyber-physical system malfunction;
4) Hazards created in the vicinity of the workplace by work-related activities on or with cyber-physical systems under the control of the Company;
5) Cyber-enabled infrastructure, equipment, and materials at the workplace, whether provided by the Company or others;
6) Changes or proposed changes in the Company, its activities, or materials;
7) Modifications to the cybersecurity ship management, including temporary changes, and their impacts on system operations, cyber-enabled system processes, risk management, and risk-related activities;
8) Any applicable legal obligations relating to risk assessment and implementation of necessary controls that affect either personnel, the ship or asset, or the outside environment;
9) The design of work areas, human work processes, cyber-physical system operations, system installations, machinery/equipment present, operating procedures, and work organization, including their adaptation to human capabilities (Note: modelled on OHSAS 18001:2007 4.3.1); and
10) Any potential environmental conditions that would affect existing cyber-enabled systems and procedures (e.g., environmentally-caused system failure), or Cyber Safety-related conditions or procedures, such as if disaster event recovery efforts required all wireless network access points to be made open-access for recovery workers.

3.2 Methodology

The Company's methodology for cyber-physical system hazard identification and risk assessment is to be defined with respect to its scope, nature, and timing to confirm it is proactive rather than reactive and provide for the identification, prioritization, and documentation of cyber-enabled system risks and the application of controls for either local and remote access or operation, as appropriate.

3.3 Management of Change

For the management of change, the Company is to identify the cybersecurity hazards and cyber physical system operational risks associated with changes in the Company, the cybersecurity ship management, or its activities, prior to the introduction of such changes.

3.4 Assessment Results

The Company is to confirm that the results of these assessments are considered when determining controls.

3.5 Cybersecurity Controls

When determining cybersecurity controls, or considering changes to existing cybersecurity controls, consideration shall be given to reducing understood or potential risks according to the following hierarchy:

1) Elimination
2) Substitution
3) Engineering controls or mitigation actions
4) Signage/warnings and/or administrative controls
5) Personal protective equipment

6) Transference of the risk, or sharing of the risk with other entities that may share supervisory or monitoring responsibilities with the Company

3.6 Functional Specification Document

The Company shall document and keep the results of identification of hazards, risk assessments and determined controls up-to-date in the Risk Management Plan and/or in the Functional Specification Document (FSD). Section 1.C.3, Fig. 1.1 Capability assessment process lists expected documents and artefacts to include within the FSD.

3.6 Cyber-physical System Risks and Controls

The Company is to confirm that the cyber-physical system risks and determined controls are taken into account when establishing, implementing, and maintaining its cybersecurity ship management.

4. Legal and Other Requirements

4.1 Documented Procedure

The Company is to establish, implement, and maintain a documented procedure:

1) To identify mandatory rules and regulations applicable to both ship and shore-based operations;
2) To identify applicable codes, guidelines, and standards recommended by the IMO, Administrations, classification societies, and maritime or control system industry organizations;
3) For identifying and accessing the legal and other requirements to which the Company subscribes that are applicable to its cybersecurity compliance requirements; and
4) For periodically evaluating compliance at least once every 12 months with applicable legal or regulatory requirements for cybersecurity, and other requirements to which the Company subscribes. The Company shall keep records of the results of the periodic evaluations in the Risk Management Plan and/or in the Functional Specification Document (FSD).

4.2 Legal and Other Requirements

The Company is to take into account applicable legal requirements and other requirements to which the Company subscribes in establishing, implementing and maintaining its cybersecurity management system. The Company is to review the legal and other requirements at least once every 12 months and keep this information up-to-date in the Risk Management Plan and/or in the Functional Specification Document (FSD).

5. Cybersecurity Baseline

The Company is to establish a cybersecurity baseline using the information in the initial BKI review, considering the Company's cybersecurity posture and findings of the review. Changes in cybersecurity posture are to be measured against the cybersecurity baseline and tracked or managed in the cybersecurity management plan, or if appropriate, in the Risk Management Plan and/or in the Functional Specification Document (FSD).

6. Management Programs

6.1 General

The Company is to establish, implement, and maintain programs for achieving its objectives and targets taking into account the unique design characteristics and operating requirements of each ship type, its cyber-enabled systems, its cyber-physical (control) systems, and their potential effects both on board and off board the ship or asset.

The Company shall determine the processes needed for the cybersecurity ship management and their application throughout the Company. The Company is to determine the sequence and interaction of these processes. The programs are to:

1) Identify criteria, methods, resources, and information required to effectively monitor, measure where applicable, analyse, control, and implement the identified processes in operating the cybersecurity management system, or its related safety or environmental impact control processes;
2) Include defined levels of responsibility and authority and lines of communication between, and amongst, shore and shipboard personnel in expected aspects of cyber-enabled or cyber-physical system operations;
3) Include the means, responsibility assignments and time frame by which the objectives and targets of the cybersecurity management system are to be achieved, including parameters to be monitored, and casualty control reaction procedures or processes identified and documented;
4) Be reviewed at regular and planned intervals and updated as necessary, so that objectives are achieved.

These processes are to be managed by the Company in accordance with the requirements of this Guidelines. Where the Company "chooses to outsource any process that affects product conformity to requirements, the Company shall confirm control over such processes. The type and extent of control to be applied to these outsourced processes shall be defined within the management system". (ISO 9001:2015, 4.1)

7. Cybersecurity Ship Management Documentation

The Company is to describe the appropriate cybersecurity-related security, health, safety, or environmental protection program effects or impacts, within the management system documentation, as applicable. Each and every cyber-physical system with potential impacts on health, safety or environment is to be documented.

7.1 Cyber-physical System Documentation

The cybersecurity management system documentation is to:

1) Define and document the scope of the cybersecurity ship management including detail and justification for any exclusions;
2) Include appropriate Company policies, objectives and targets;
3) Define the responsibility, authority, and interrelation of the personnel who manage, perform, and verify work relating to and affecting cyber-physical system security or cybersecurity, safety operations, or environmental effects, as appropriate;
4) Describe the core elements and outline the structure of the Company's cybersecurity ship management and interaction of its elements, and reference to related documents;
5) Include documented procedures established for the cybersecurity management system or provide appropriate references to cybersecurity ship management documentation. The complexity of the work and the skill level of personnel involved in performing the work and the work environment shall govern the degree of control provided within management system procedures;
6) Describe the interaction between the processes of the cybersecurity ship management, indicating any dependencies or critical enabling factors that must be considered;
7) Include the procedures and records required by this Guide to demonstrate conformity to Cybersecurity level requirements and the effective planning, operation, and control of the cybersecurity ship management processes.

8) Include documents, including records, determined by the Company to be necessary to demonstrate the effective planning, operation, and control of processes that relate to its significant Cybersecurity aspects and management of its cybersecurity risks to both IT and OT systems; and
9) Be kept in the form that the Company considers most effective in the cybersecurity ship management plan, the Risk Management Plan and/or in the Functional Specification Document (FSD).

B. Implementation and Operation

1. Resources, Roles, Responsibility, Accountability, and Authority

1.1 Resources

The Company's top management is to determine and provide the resources essential to establish, implement, maintain, and improve the cybersecurity management system. Resources include human resources and specialized skills, organizational infrastructure, technology, and financial resources. Resources also include personnel suitably trained to perform verification activities including internal management system or cybersecurity audits.

1.2 Roles and Responsibilities

The Company's management is to demonstrate its commitment by defining roles, allocating responsibilities and accountabilities, and delegating authorities, to facilitate effective cybersecurity ship management. Roles, responsibilities, accountabilities and authorities are to be defined, documented, and communicated. All those with management responsibility are to demonstrate their commitment to the continual improvement of cybersecurity performance. Top management it to take ultimate responsibility for cybersecurity and the cybersecurity ship management.

2. Master's Responsibility and Authority

The Company is to clearly define and document the Master's responsibility with regard to: (Adapted from ISM 5.1):

1) Implementing the security controls designated for use with cyber-enabled and cyber-physical systems in accordance with policy of the Company;
2) Motivating the crew to observe that policy;
3) Issuing appropriate orders and instructions in a clear and simple manner;
4) Verifying that specified requirements are observed; and
5) Periodically reviewing the cybersecurity ship management and reporting its satisfactory performance or its deficiencies to the shore-based management.

The Company is to confirm that the cybersecurity ship management operating on board the ship contains a clear statement emphasizing the Master's authority. The Company establishes in the cybersecurity ship management that the Master has the overriding authority and the responsibility to make decisions with respect to personnel, system, ship or asset security, safety and pollution prevention, and to request the Company's assistance as may be necessary. (Adapted from ISM 5.2)

3. Shipboard Personnel

3.1 Master's Qualification and Support

The Company shall confirm that the Master is (Adapted from ISM 6.1):

1) Properly qualified for command;
2) Fully conversant with Company's cybersecurity management system; and
3) Given the necessary support so that the Master's duties can be effectively performed in ensuring the Cyber Safety of the ship, its systems, and its cyber-physical functions.

3.2 Crew

The Company is to establish procedures to confirm that new personnel and personnel transferred to new assignments related to cyber-physical systems, their safety and security, and protection of cyber-enabled systems that could affect the environment, are given proper familiarization with their duties. Instructions which are essential to be provided prior to sailing should be identified, documented and given." (Adapted from ISM 6.3)

The Company is to establish procedures by which the ship's personnel receive relevant information on the cybersecurity ship management in a working language or languages understood by them. (Adapted from ISM 6.6)

The Company is to confirm that the ship's personnel are able to communicate effectively in the execution of their duties related to the cybersecurity management system. (Adapted from ISM 6.7)

The Company is to confirm that persons in the workplace take responsibility for aspects of cybersecurity over which they have control, including adherence to the Company's applicable cybersecurity requirements.

4. Control of Documents

4.1 Cybersecurity Ship Management Documentation

Cybersecurity Ship Management documentation consists of:

1) Established, implemented, and documented procedures for:
   A) Policy and procedural document and data control, including documents of external origin;
   B) Security or cybersecurity internal audits;
   C) Security-related corrective and preventive action;
   D) System non-conformances, declared incidents, hazardous occurrences and near misses;
   E) Control of system testing and quality records;
2) Documented system or application test (quality) policy and security testing objectives;
3) A testing and system quality manual;
4) Documents required for effective planning, operation and control of its processes; and
5) Records required to demonstrate compliance with requirements and of effective operation of the management system. (Note: The documentation can be in any form or type of medium)

5. Operational Control

5.1 Shipboard Cyber-related Operations

The Company is to establish procedures, plans and instructions, including checklists as appropriate, for key shore-based and shipboard cyber-related operations and activities concerning the safety of personnel, safety of the ship, prevention of pollution, or other activities that can be affected by software-intensive or cyber-physical systems, in support of the Company policy, objectives, targets and action plans. The various tasks are to be defined and assigned to qualified personnel.

5.2 Flag State

The Company is to establish, implement, and maintain documented instructions and procedures to promote cyber-safe operation of ships, offshore assets and the associated shore facilities and protection of the environment in compliance with relevant International and National regulations.

5.3 Controlled Conditions

The Company is to identify those operations and activities that are associated with identified hazards and significant cyber-enabled system risk areas where control measures need to be applied to manage the risks. Such controls include software management of change. The Company is to plan these operations and activities in order that they are carried out under controlled conditions. The output of this planning is to be in the form suitable for the Company's method of operations. Controlled conditions include:

1) Compliance with mandatory rules, regulations, and codes;
2) Established and maintained documented procedures/work instructions to control situations where their absence could lead to deviation from the policies, objectives, and targets;
3) Defined tasks assigned to properly qualified personnel;
4) The Company's permit to work systems, which shall include measures to verify that the condition of spaces and systems as safe or not safe for work is readily identifiable. These measures shall also include safeguards so that work does not proceed unless safe conditions exist. The condition of spaces or systems being worked on shall be updated as appropriate throughout the course of the work;
5) Supply chain controls related to purchased goods, equipment, and services;
6) Third party access controls related to contractors and other visitors to the workplace;
7) The availability of suitable monitoring and measuring equipment;
8) Implementation of monitoring and measurement; and
9) Validation of approved processes and equipment, as appropriate, and required records

This page intentionally left blank

Section 4 Requirements for Cybersecurity System

A. General

This section gives the information regarding the requirement for cybersecurity notation, certification of cybersecurity system as well as cybersecurity level. Requirements for cybersecurity notation and assessment of cybersecurity system is described in B. Furthermore, for each cybersecurity level (Informed, Advanced, Adaptive) will be explained in C, D, and E, respectively. Implementation for Information Technology (IT) and Operational Technology (OT) as well as additional requirements for each specific cybersecurity level will be explained in F.

B. Requirements for Cybersecurity Notation or Certification of Cybersecurity System

The procedure and requirements for Cybersecurity as explained in C to F is to be built and provided by the company. These procedure and requirements provide continuous support for the security facets appropriate to the Company's security strategy. BKI will assess the scope and depth of the implementation of those requirements. A company under assessment for specific cybersecurity level is to demonstrate that:

1) The requirements correspond to selected cybersecurity level are provided, supported and maintained by the Company;
2) The Company has implemented further requirements – even if they are not part of the assessment process in consideration – to confirm completeness of security;
3) The requirements and its related specifications for Operational Technology have been applied where appropriate for the process control and OT aspects of its architecture that have contact with, or impact upon, human safety-related conditions; and
4) The security specifications, conditions and controls applicable under specific requirements are implemented and monitored as required to maintain security appropriate to the risk conditions understood in the Company.

It is essential to understand that building and sustaining the requirements will require governance guidelines for consistent maintenance which can be elaborated as follows:

– The security prioritization efforts across Company can be achieved with the security levels provided in this Guidelines. Security requirements for any particular organization must be tailored to its individual conditions, assets to be protected, risk conditions, and security threats. Prospective company may choose to certify at Informed level, while needing to provide security from procedures and requirements in the Advanced level as well.
– Procedures and requirements determine effective application of security controls and techniques. Its determine effectiveness and sustainability of security measures in place in any Company's environment.

– A Company with assets or operational needs in excess of its given security level of certification, may require policy statements to guide their employees and system users that exceed minimum requirements for their security level.

C. Cybersecurity Level 1 - Informed Cybersecurity

The requirements for the compliance with the Cybersecurity Level 1 - Informed Cybersecurity are indicated in this Sub-Section.

The guidance for implementation and additional requirements related to IT and OT are set out in E.

1. Asset Management

1.1 Following requirements related to asset management as applicable are to be defined and implemented:

- The ship is to identify various processes required for its operations and make a detailed inventory of all information technology (IT) and operational technology (OT) systems.
- The inventory of asset is to include identification of application software, operating system software and various types of network communications in main and sub systems.
- Request for asset changes are to be approved and documented.
- Where the version number/model number of the asset under replacement is different from the installed asset, the configuration of the new asset to meet the desired functional requirements, is to be evaluated prior to installation.
- Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools
- Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
- Critical cyber systems (IT and OT) which when attacked can affect its business, vessel/ offshore asset safety and environment are to be identified;
- All external communication paths to its cyber systems are to be identified and mapped;
- All networks including network devices in the ship are to be inventoried;
- Critical areas having sensitive information and appropriate access control measures are to be identified;
- Systems, loss of which can have impact on critical nature of business undertaken by the ship, are to be identified;
- Hardware, Software, devices and data are to be prioritized based on their criticality.

2. Governance

2.1 Policies and procedures towards implementation of a cyber-safety management system are to be defined. A Cyber safety policy is to be established, implemented and maintained. There is to be a general awareness of cyber risk at senior management level.

2.2 A Ship Cyber Safety Officer (SCSO) is to be identified and nominated. The main responsibilities of the SCSO are to include implementation of the approved cyber safety program and monitoring the effectiveness of the same.

2.3 As shore support is important for implementation of Cyber safety on board a vessel, designating a company shore based Cyber security officer is recommended. The Ship Cyber security officer can be supported by Company Cyber security officer for providing on shore support on Cyber safety issues.

2.4 Following requirements as applicable are to be defined, documented and implemented towards an effective governance:

- A business continuity plan in the event of cyber-attack on critical systems;
- A cyber safety policy for the ship;
- Clear definition of roles and responsibilities with regard to cyber safety;
- Legal and regulatory obligations/ requirements with respect to Cyber safety are to be identified;
- The senior management and employees working on critical cyber systems are to have general awareness on cyber safety;
- Ship cyber safety officer is to be designated who would be responsible for implementation of cyber safety programme
- Procedure for monitoring of regulatory requirements and addressing them is to be formulated.

3. Risk Assessment

3.1 A detailed risk assessment is to be carried out before implementing normal protection devices such as fire walls, antivirus etc. The risk assessment is to be carried out to assess the safety, environmental effects and business risks due to cyber-attack. The results of risk assessment are to be used to ensure that appropriate measures are selected, and the systems are protected in proportion to the risk.

3.2 The Risk assessment and analysis is to be carried out to arrive at risk value for an identified vulnerable system. ISO 31000 or equivalent standard may be referred for the risk analysis. The risk assessment process is to have methods to prioritize the vulnerabilities. The results of physical, health safety and environment (HSE) and cyber safety risk assessments are to be integrated to arrive at overall risk.

3.3 Vulnerability assessments of critical systems and potential threats that the ship can face are to be documented. The process involves identification of all systems which when attacked, can result in partial or full compromise of the ship's safety and/ or its impact on environment.

3.4 A list of typical onboard vulnerable systems on a Ship is indicated below. The list is indicative and exact list would depend on the type of vessel and its operational requirements):

- Cargo management systems.
- Bridge systems.
- Propulsion Control system
- Machinery Control system
- Power control systems.
- Watertight door systems
- Passenger servicing systems
- Fixed or wireless networks connected to the internet installed on board for the benefit of passengers
- Administrative and crew welfare systems
- Communication systems.

3.5 The risk assessment document, as a minimum, is to address the following requirements:

- Established risk acceptance criterion;
- Identification and documentation of consequences of each threat on vulnerable system;
- Approved and documented risk methodology;
- Identification of risk priorities based on severity of impact;
- Risk classification

- Identify risks which can be mitigated / accepted.

4. Physical and System Access Control

4.1 Access control systems are to be implemented to restrict the entry of personnel to areas where critical assets are located. For e.g. propulsion control systems, computer systems for ship shore communication, bridge navigation systems, etc. The physical environment may be monitored for cyber-security events.

4.2 The access control may be implemented area wise e.g. where only authorized personnel are allowed to enter the area. This could be implemented through a smart card or bio metric systems which allows only authorized personnel to enter into a work area.

4.3 The ship is to define procedures and implement system access controls. The ac-cess control can be network based where only authorized personnel are given rights to enter or can be system based, where the system allows only a particular user to log in. A combination of both the systems is recommended in line with the risk analysis.

4.4 The selected control is to be suitable for the type of system i.e. Information Technology (IT) / Operation Technology (OT). Following controls as applicable are to be implemented:

- Barriers to prevent unauthorized access into critical systems;
- The ship is to formulate a policy on removable media;
- Implemented Controls are to be suitable for the type of system i.e. information technology or operation technology;
- Safety levels required for systems/ equipment based on risk assessment are to be identified and implemented;
- Physical access control is to be provided in areas where Cyber systems essential for ship operation are installed;
- The administrative controls for system log are to be implemented;
- Measures to ensure Endpoint Security are to be implemented;
- Removable media is protected and its use restricted according to policy;
- Policy to limit the use of external devices e.g. USB devices is to be formulated and implemented;
- The control system is to provide the capability to uniquely identify and authenticate all human users;
- Access accounts are to be role based to manage access to appropriate in-formation or systems for that user’s role;
- The allocation of privileged access rights is to be restricted and controlled.

5. Network Security

5.1 A Network plan clearly identifying all the network components for each on board IT and OT network is to be submitted.

5.2 The IT and OT networks are to be protected against unauthorized access from both internal and external sources through implementation of suitable controls. Physical layout of network components is to be considered in implementation of suitable physical access control.

5.3 Following requirements as applicable are to be complied with:

- The internet access is not to be directly connected to ship network
- Users shall only be provided with access to the network and network services that they have been specifically authorized to use

- Perimeter security is to be provided through suitably configured fire walls. The fire wall configurations is to be in accordance with organization risk management policy.
- The network is to be monitored to detect cyber incident

6. System security controls

6.1 The procedure and controls for detecting a Cyber incident is to be defined and implemented. The detected events are to be analyzed.

6.2 The selected control is to be suitable for the type of system i.e. Information Technology (IT) / Operation Technology (OT).

6.3 Following controls and procedures are to be implemented as applicable:

- Roles and responsibilities for detection are to be defined;
- The physical environment is to be monitored to detect potential cybersecurity events;
- Malicious event is to be detected
- Event logs are to be analyzed.

7. Detection Procedures

7.1 The procedure and controls for detecting a Cyber incident is to be defined and implemented. The detected events are to be analyzed.

7.2 The selected control is to be suitable for the type of system i.e. Information Technology (IT) / Operation Technology (OT).

7.3 Following controls and procedures are to be implemented as applicable:

- Roles and responsibilities for detection are to be defined;
- The physical environment is to be monitored to detect potential cybersecurity events;
- Malicious event is to be detected
- Event logs are to be analyzed.

8. Training, awareness & information sharing

8.1 Senior management on board, are to be aware of cyber safety issues and sufficient training is to be imparted to all personnel involved with Cyber- Safety.

The cyber safety awareness may be increased using following methods but not limited to:

- Email communications;
- Newsletters;
- Videos and DVDs;
- Websites and webcasts.

8.2 Following requirements are to be complied with, as applicable, towards an effective Cyber safety awareness:

- Key senior personnel who would be involved in top level decisions towards cyber safety implementation are to be identified and communicated;
- Cyber safety training needs relevant to the job are to be identified;
- Mechanism to capture changes in cyber regulatory policies is to be in place;

- Cyber information is to be shared in an informal way, except in critical/emergency condition.

9. Response and Recovery Procedures

9.1 A cyber incident response and backup procedure document is to be prepared. Following requirements are to be complied with, as applicable:

- Methods are to be established and documented for responding to an incident;
- Persons responsible for incident response and back-up are to be clearly identified and their roles defined;
- Each incident is to be recorded and reviewed periodically for lessons learnt;
- Location of software and hardware required for backups are to be documented and inventoried;
- Location of back-up storage, authorization for retrieval for backups are to be defined and documented;

9.2 A back-up policy in the event of cyber system being compromised is to be documented along with procedures for implementation. The document is also to indicate the roles and responsibilities of persons involved;

- Procedure for escalating unresolved problems is to be formulated.
- The information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan are to be addressed.
- Events are to be reported consistent with established criteria

9.3 Communications

Personnel know their roles and order of operations when a response is needed

- Incidents are reported consistent with established criteria
- Information is shared consistent with response plans
- Coordination with stakeholders occurs consistent with response plans
- Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness
- Public relations are managed
- Reputation is repaired after an incident
- Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

10. Cyber Safety Process Review

10.1 Review of the risk assessment and mitigation controls is to be carried out upon any addition of new asset or change in model /make of asset of the risk assessment and mitigation controls is to be carried out upon any addition of new asset or change in model /make of asset.

10.2 The revised policies and procedures are to be approved.

D. Cybersecurity Level 2 - Advanced Cybersecurity

The requirements for the compliance with the Cybersecurity Level 2 - Advanced Cybersecurity are indicated in this Sub-Section. These are to be complied with, in addition to the requirements for Cybersecurity Level 1.

The guidance for implementation and additional requirements related to IT and OT are set out in E.

1. Asset Management

1.1 The asset registry is to be reviewed and updated with every:

- change in operation area;
- change of flag;
- change of class;
- changes in its IT or OT systems

1.2 The ship is to formulate a procedure for patch management. Patch management tasks include maintaining current knowledge of available patches, identify patches appropriate for particular systems and ensure installation of patches in accordance with manufacturer recommendations.

1.3 The updated software is to be tested and the asset registry is to be updated.

1.4 Following requirements are to be complied with as applicable:

- Replaced assets are to be verified with base line configurations;
- Asset changes are to be managed;
- Assets are to be prioritized;
- The asset inventory is to be current;
- Firmware is to be updated as per manufacturer recommendations and updated asset is to be tested. When the asset forms a part of an integrated system, then the complete integrated system is to be tested.

2. Governance

2.1 The policies and procedures are to be reviewed periodically and the revised approved policies are to be communicated to all concerned. The review periodicity is to be defined.

2.2 Procedures are to be established and reviewed with respect to the addition, removal and disposal of all assets.

2.3 The implemented controls are to be verified towards compliance to requirements indicated in this section. The results of verification are to be considered during re-view of policies and procedures.

3. Risk Assessment

3.1 Internal threat information, now detected and analysed by the detection process, are to be considered in the risk assessment.

3.2 A vulnerability scan is to be performed on IT systems. For carrying out vulnerability testing of OT systems, manufacturer consent is to be obtained and is ad-vised to be carried out during berthing. The results of above tests and information received from external sources on known vulnerability are to be considered during risk assessment.

3.3 Documented and approved Procedures and processes to carry out risk assessment and the controls implemented towards risk mitigation of ship’s IT and OT systems are to be reviewed and updated as required

- Risks indicators and threats are to be regularly reviewed and updated where found necessary;
- Any new identified threats are to be documented and risk analysis is to be carried out;

- Each cyber safety related incident is to be recorded and reviewed periodically for lessons learnt;
- Information about technical vulnerabilities of information systems being used are to be obtained in a timely fashion, the ship's exposure to such vulnerabilities is to be evaluated and appropriate measures taken to address the associated risk;
- Periodic reviews of risk management process for IT and OT systems are to be carried out. The document is to define the periodicity of review;
- Risk responses are to be identified and prioritized;
- Methods are to be formulated and implemented to assess and address da-ta integrity risks;
- Consequences of accepted and residual risks are to be reviewed periodically

4. Physical and System Access Control

4.1 Access control measures are to be reviewed periodically. Detected access breach incidents are to be considered in review.

4.2 Suitable measures are to be identified and implemented to address the Identified issues.

4.3 Base line authentication procedures for remote users is to be implemented. The ship is to area specific system authorization.

5. Network Security

5.1 In addition to perimeter security and creation of Demilitarised Zone (DMZs), the network security is to be augmented by provision of VPNs and VLANs.

5.2 Formal transfer policies, procedures and controls are to be in place to protect the transfer of information through the use of all types of communication facilities.

5.3 The control system is to provide the capability to deny external network traffic by default and allow network traffic by exception.

5.4 Communication and control networks are to be protected.

5.5 The ship is to implement a suitable security monitoring method and a procedure to determine the impact of events is to be established. Following methods may be used as applicable:

1) Intrusion Detection Systems (IDS) based on signature matching algorithms. The systems can be network based or specific to one equipment.
   - Network based intrusion detection is to identify unauthorized, illicit, and anomalous behavior based solely on network traffic. The role of a network IDS is passive, only gathering, identifying, logging and alerting.
   - Host based intrusion detection system (HIDS), is to identify unauthorized, illicit and anomalous behavior on a specific device The role of a host IDS is passive, only gathering, identifying, logging, and alerting.
   - Physical intrusion detection is the act of identifying threats to physical systems. Physical intrusion detection systems may act as prevention systems. Examples of Physical intrusion detections may be
     a) Security Guards
     b) Security Cameras
     c) Access Control Systems (Card, Biometric)
     d) Motion Sensors

2) Intrusion prevention has the same process of gathering and identifying data and behavior, with the added ability to block (prevent) the activity. This can be implemented with Network, Host, or Physical intrusion detection systems.

3) Following requirements are to be complied with as applicable:

- Procedures are to be in place to assess the requirements of detection process when any new system is added/ replaced;
- Process for various types of detection methods based on criticality and vulnerability of the systems are identified by the ship;
- Incident thresholds are to be established.
- The ship is to have a policy to maintain network integrity;

6. System security controls

6.1 Data Security

6.1.1 The ship is to implement suitable controls to ensure data security.

6.1.2 Each time data is replicated or transferred, it is to remain intact and unaltered between updates.

6.1.3 Error checking methods and validation procedures are to ensure the integrity of data that is transferred or reproduced without the intention of alteration.

6.1.4 Data integrity may be compromised in a number of ways:

- Human error, whether malicious or unintentional;
- Transfer errors, including unintended alterations or data compromise during transfer from one device to another;
- Bugs, viruses/ malware, hacking and other cyber threats;
- Compromised hardware, such as a device or disk crash;
- Physical compromise to devices.

6.1.5 Data security is one of several measures which can be employed to maintain data integrity, as unauthorized access to sensitive data can lead to corruption or modification of records and data loss.

6.1.6 Following requirements are to be complied with as applicable, towards ensuring data security:

- Policies and procedures for management of information data in accordance with its defined risk strategy are to be developed;
- Procedures to store confidential data and protect it from unauthorized access are to be developed;
- Back-up procedures for critical data are to be identified;
- Procedures to protect data in transit and data at rest are to be developed and implemented;
- The control system is to provide the capability to protect integrity of sessions and is to reject any usage of invalid session IDs;
- Procedures are to be implemented to control the installation of software on operational systems;
- Detection, prevention and recovery controls to protect against malware are to be implemented.

6.2 Information protection

6.2.1 The processes and procedures for information protection are to be established.

6.2.2 Security policies clearly identifying the purpose, scope, roles, responsibilities and coordination are to be established.

6.2.3 Following requirements are to be complied with, as applicable:

- A baseline configuration for IT systems is to be defined;
- A baseline configuration for OT systems is to be defined;
- A system development life cycle to manage systems is to be implemented;
- Configuration change control process is to be established;
- Systems backup are to be taken at clearly defined back up period.
- Procedure for testing the backs ups is to be established;
- The physical operating environment for various IT and OT assets are to be established and documented;
- Process and procedure for destruction of data is to be clearly de-fined;
- A process to continually improve the protection process is to be available;
- Incident response plans are to be established;
- Incident recovery plans are to be established;
- Disaster recovery plans are to be established;
- Procedures and processes for testing response and recovery plans are to be available;
- Practices to include cyber safety issues in human resources practices e.g. personnel screening are to be established;
- Vulnerability management plan is to be established and implemented;
- Access to systems and assets is to be controlled, incorporating the principle of least functionality

7. Detection Procedures

7.1 Advanced threat Detection techniques ex. Anomaly Detection (AD) and Network Behavior Anomaly Detection (NBAD) are to be implemented for threat detection.

7.2 Network Behavior Anomaly Detection (NBAD) approach may be used to network security threat detection. NBAD is the continuous monitoring of a network for unusual events or trends.

7.3 An NBAD program is to track critical network characteristics in real time and generate an alarm if a strange event or trend is detected that could indicate the presence of a threat. Large-scale examples of such characteristics may include traffic volume, high bandwidth use etc.

7.4 NBAD solutions may also be used to monitor the behavior of individual network subscribers. NBAD is to be used in addition to conventional firewalls and applications for the detection of malware.

7.5 A cyber safety center is to be setup in a suitable location from where all the cyber safety issues, monitoring of various cyber safety parameters, access control, business continuity, disaster management can be supervised/ controlled by suitable designated person

7.6 The cyber safety center may be supported by shore based security operations center. In such cases the logs generated by the ship are to be forwarded to the SOC for analysis and for further instructions/advice to ship. The SOC may act as centralized nodal point for fleet of ships to address cyber issues.

7.7 Following requirements for threat detection are to be complied with, as applicable:

- Procedures and controls are to be defined and implemented to detect and analyze anomalous activities in timely manner;
- Procedure to analyze the behavior of individual network traffic to form a base line is to be defined;
- Potential impacts of detected anomalies are to be identified;
- All IT and OT systems are to be monitored at regular intervals for unusual activities and breaches;
- Procedures for communication and immediate action when an anomaly is detected are to be formulated;
- Implementation of detection process such as fire walls, intrusion detection and prevention systems to identify threats;
- Periodically evaluate overall security management system to ensure the security objectives are met and detection processes are continuously improved;
- Investigation of notifications from detection systems is to be undertaken

8. Training, awareness & information sharing

8.1 The security of process control systems is to be improved by increasing awareness, improving skills and techniques

8.2 Cyber safety awareness programs are to provide insights into threats and risks to various control systems including the technical and procedural solutions that can be deployed to prevent cyber safety attacks from succeeding.

8.3 The training is to cover a wide technical area, ranging from IT skills to process control skills. Organizations are to develop customized training frameworks to ensure that personnel have the appropriate skills and knowledge to perform their jobs securely.

8.4 A training framework is to be developed that covers training for the key personnel, detailing the level of understanding of an organization’s vulnerabilities, the information and resources that can be accessed to share good practices and approved mitigation measures.

8.5 Following requirements are to be complied with, as applicable:

- Process to update its senior management on impact of cyber risks on legal and business aspects are to be defined;
- A formal process to identify the training need by the line manager is to be in place;
- Provision is to be made for subject matter external experts for training;
- Training requirements, that address internal threats, lessons learnt and external cyber information are to be defined;
- Specific programs to train its employees on Operation technology and Information technology are to be established;
- Effective communication of updated information on cyber safety is made to its employees through various communication media. For e.g. emails, seminars, workshops, etc.
- Procedures to implement preventive maintenance routines such as antivirus and anti-malware, patching, backups, and incidence-response planning and testing; are to be covered as part of training.

9. Response and Recovery Procedures

9.1 Response Procedures

9.1.1 Processes and procedures to identify and respond to threats are to be defined and documented.

9.1.2 The methodology of handling IT/ OT cyber incidents are to be defined.

9.1.3 Following requirements are to be complied with as applicable:

- The ship is to have Cyber Safety Response Team (CSRT) to deal with all types of cyber threats;
- The rules, roles and responsibilities of the CSRT are to be clearly defined;
- The ship is to have procedures and methods to regularly monitor and update its response plans;
- Process for early warning system and means to communicate are to be clearly defined.

9.2 Recovery Procedures

9.2.1 Effective recovery planning is a critical component of a ship/s preparedness for cyber event. Recovery planning is to enable participants to understand system dependencies, critical personnel identities such as crisis management and incident management roles, arrangements for alternate communication channels, alternate services, alternate facilities etc.

9.2.2 The planning and documentation for recovering from a cyber-security event is to be in place before the cyber event occurs.

9.2.3 Following requirements are to be complied with, as applicable:

- The ship has formulated and documented well defined recovery and back up procedures;
- Critical systems and data which need to be recovered in the event of cyber-attack are to be identified;
- Location of back up storage, authorization for retrieval for backups are to be defined and documented;
- Personnel, teams who are responsible for recovery are to be identified;
- Procedures are to be formulated to train personnel in backup and recovery process;
- Procedures for dealing with the loss or theft of unencrypted backup tapes that contain proprietary or sensitive information are to be formulated

9.3 Communication

9.3.1 The type of communication required is to be defined by the type of incident and its potential impact.

9.3.2 Communication control (both internal and external) is to ensure that right information is communicated at the right moment by the right senders to the right receivers. Controls are to address communication openness and protection.

9.3.3 A list of potential stakeholders is to be prepared and procedures are to be defined to ensure that the right contact information is available for effective communication.

9.3.4 The ship has to identify alternative secure communication channels and the process to be followed after a cyber-incident.

9.3.5 When an actual cyber safety incident occurs, the cyber safety incident response team is to immediately draw up a concrete communication plan for the specific incident. Effective procedures towards the same are to be documented.

9.3.6 Following requirements are to be complied with as applicable:

- All the internal stake holders who need to be communicated with, in an emergency, are to be identified;
- Ways of communications for internal stake holders are to be clearly defined;
- Information required to be communicated to every person is to be clearly defined;
- All the external stake holders who are required to be communicated in emergency are to be identified;
- Mode of communication to external stakeholders is to be defined;
- Extent of information which needs to be communicated is to be defined;
- Any specific authorization required before communicating sensitive information is to be established;
- Communication to media is to be defined i.e. what to communicate and who would communicate;
- Redundant communication paths, in the event of loss of primary communication path are to be identified.
- The ship is to have a documented contingency plan.

10. Cyber Safety Process Review

10.1 The cyber safety technical controls and procedures are to be reviewed periodically. The periodicity level is to be defined,

10.2 The threat information results received from the analysis of detected threats, is to be considered in the review process.

10.3 Threat information from similar industries received from various forums is to be considered in risk analysis.

E. Cybersecurity Level 3 - Adaptive Cybersecurity

The requirements for the compliance with the Cybersecurity Level 3 - Adaptive Cybersecurity are indicated in this Sub-Section. These are to be complied with, in addition to the requirements for Cybersecurity Level 2. The guidance for implementation and additional requirements related to IT and OT are set out in E.

1. Asset Management

1.1 The asset registry is to include all the ship IT, OT assets and associated networks.

1.2 Asset registry is to be reviewed periodically and upon any change of asset configuration, or upgradation due to evolving technology.

2. Governance

2.1 The security of process control systems can be at risk by third parties e.g. vendors, service suppliers, maintenance supports teams etc. which interact with ship’s cyber systems.

2.2 Following requirements are to be complied with as applicable:

- All the third party vendors, service providers who interact with the ship cyber systems are to be identified;
- An agreement with third party insisting on implementation of basic cyber safe-ty control such as fire walls, antivirus etc. at their end is to be formulated;
- Patch updating process with third party software providers is to be formulated;
- Responsibilities of third party are to be clearly defined;
- Specific clauses in contract with third party to manage cyber risk are to be included. Typical clauses are to include non-disclosure agreement, immediate communication on any detected risk by the third party which can affect the ship.

3. Risk Assessment

3.1 Penetration Testing

External penetration testing is required to be conducted to identify weaknesses in the ship's network which could allow an attacker to access the systems. Special care is to be taken when performing penetration tests on live (in-production) systems. Penetration testing is to be considered especially when employing new technology or processes as well as when the risk picture has changed.

Following requirements are to be complied with as applicable:

- Goals for penetration testing are to be clearly defined and the same is to be communicated to the test team;
- The network architecture is to be evaluated for an appropriate defence-in-depth security strategy;
- A strategy for using firewalls is to be developed and functional demilitarized zone (DMZs) are to be established;
- Information which can be shared with test team as per the desired mode of testing i.e. black box, grey box or white box testing, is to be clearly de-fined.

4. Physical and System Access Control

4.1 The ship is to implement advanced authentication controls. For system access.

4.2 Physical and system access can be implemented function specific or zone specific.

4.3 The procedures and controls are to reviewed periodically. Information new threat, breaches are to be analysed and existing process is to be reviewed/updated as required.

5. Network Security

The controls used for the detection process are to be regularly updated and tested in line with latest technology

5.1 Network Segmentation

5.1.1 Network segmentation involves apportioning of networks into small networks with clearly defined rules on which systems/ users can communicate from/ to a network. This may be achieved by:

- Division of large networks into separate network domains (segments);
- Consideration of physical and logical segregation;
- Definition of domain perimeters;
- Definition of traffic rules between domains;

- Usage of authentication, encryption, and user-level network access control technologies.

5.2 Mobile Device Security

5.2.1 When the ship control system and network systems can be accessed from a mobile control are to be implemented for a secured connectivity. Following requirements are to be complied with as applicable:

- Usage restrictions and implementation guidance for ship controlled portable and mobile devices are to be formulated;
- Connection of mobile devices is to be authorized meeting defined usage restrictions and implementation guidance;
- Monitoring for unauthorized connections of mobile devices to ship information systems is to be undertaken.

5.3 Wireless Device Security

5.3.1 The control system is to provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication. Following requirements towards wireless device security are to be complied with, as applicable:

- Usage restrictions and implementation guidance for wireless access are to be established;
- Unauthorized wireless access to the information system is to be monitored;
- Wireless access to the information system prior to connection is to be authorized.

6. System security controls

6.1 Cryptography

The system is to have the capability to protect the confidentiality of information at rest, during remote access sessions and during traversing of an untrusted network is to be provided. Encryption is a common mechanism for ensuring information confidentiality.

7. Detection Procedures

7.1 Advanced technological tools in the field of computer security, security information and event management (SIEM) software products are to be implemented. The SIEM combines the services of security information management (SIM) and security event management (SEM) to provide real-time analysis of security alerts generated by network hardware and applications

7.2 Monitoring system and network for changes, anomalous behaviors, or for attack signatures are essential to the Defence-in-Depth concept of protecting critical assets.

7.3 Security information management (SIM) and security event management (SEM) are to be implemented. They provide real-time analysis of security alerts generated by network hardware and applications. The network is to be monitored on a continuous basis.

7.4 Procedure for monitoring external service providers' activity and monitoring of unauthorized personnel connections is to be developed and implemented.

- Activity of external service provider is to be monitored to detect potential cyber security events;
- Monitoring for unauthorized personnel, connections, devices, and software is to be performed;

7.5 Cyber Safety Center

The control system is to provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner

8. Training, awareness & information sharing

8.1 All the personnel involved in cyber safety including the third party stake holders are to be trained to perform the designated duties related to ship cyber systems.

8.2 The training is to include evolving technologies, new threat perception from industry and risk approach methods.

8.3 The personnel involved in analysis of event logs and operation of SIEM are to be trained for use and operation of SIEM tools.

8.4 Evolving Technologies and Information Sharing

8.4.1 Cyber Safety is a dynamic subject and procedures are to be in place to keep the ship staff technically updated on new technologies, new threats and industry feedback. In the larger context, procedure to share its cyber related incidents with others and at same time learn from industry is to be formulated and implemented.

8.4.2 A holistic view of the total environment which includes external factors needs to be taken into account in this level of implementation. Examples of external context may include:

- Changes which can effect ship operations;
- Evolving technological changes which effect vessel efficiency.

8.4.3 Following requirements are to be implemented as applicable:

- Receipt of information that enables collaboration and risk-based management decisions in response to events is to be ensured;
- Position in critical infrastructure and its industry sector is to be identified;
- Mission, objectives and activities are to be prioritized and established;
- Dependencies on critical infrastructure and critical services are to be established;
- Resilience requirements to support critical infrastructure are to be identified and communicated;
- Risks are to be managed and information is to be actively shared to ensure that accurate, current information is distributed and consumed to improve cyber safety before a cyber-security event occurs;
- Critical information system components and functions are to be identified by performing a criticality analysis;
- Knowledge of its role in the larger ecosystem but has formalized its capabilities to interact and share information externally.
- Processes to train on cyber risks in relation to the physical presence of non-ship personnel, e.g. where third-party technicians are left to work on equipment without supervision are to be established;

9. Response and Recovery Procedures

9.1 A disaster recovery plan is to be formulated, approved and tested periodically. The personnel involved identified in disaster recovery plan are to be communicated about their roles and responsibilities in the event of disaster.

10. Cyber Safety Process Review

10.1 The ship has to assess its cur-rent state of implementation of cyber risk management process and is to continually work on them for further improvement.

10.2 A process to undertake continual improvement of their cyber safety systems is to be developed based on threat perception and technological changes. Following requirements are to be complied as applicable towards continual improvement:

- Prepare a current profile of ships' cyber risk practices and examine the extent to which it has progressed in implementation of cyber safety practices;
- Review its policies and procedures with respect to changes in International/ National scenarios;
- Use the above information to re-prioritize resources to strengthen other cyber safety practices;
- Consistently exhibit commitment towards cyber safety through repeated successful audits, so that cyber safety becomes an organizational culture;
- Cater for capital planning by way of budget allocation for cyber safety;
- Institute procedures to evaluate software service providers;
- Identify its business/ mission objectives and high-level organizational priorities;
- Make strategic decisions regarding cyber safety implementation and determines the scope of systems and assets that support the selected business line or process;
- A system to receive threat and vulnerability information from information sharing forums and sources is implemented;
- Take corrective action to fill the gaps through resource allocation, capital funding;
- Continuously review and improve the existing process, procedures, effectiveness, information /data security management systems;
- Carry out penetration testing to identify vulnerabilities and forensic analysis to detect and analyze cause of an attack;
- Data System is to be designed with adequate capacity;
- Formulate procedures for employee personnel data management, in addition to informational data security;
- Develop a policy addressing remote login by a user and/ or remote connections. Additional controls to automatically terminate remote access may be implemented as per the asset desired security level;
- Procedures for smart phone usage and mobile data management are to be formulated;
- Procedures are to be established and audited with respect to the addition, removal and disposal of all assets;
- Audit/ log records are to be determined, documented, implemented and reviewed in accordance with policy;
- Access to systems and assets is to be controlled, incorporating the principle of least functionality;
- The cyber-attack detection methods are to be periodically tested and continuously improved
- Event detection information is to be communicated to appropriate parties;
- Voluntary information sharing is to occur with external stakeholders to achieve broader cybersecurity situational awareness.
- Incorporate the lessons learnt and best practices from industry;

F. Guidance for Implementation and Additional requirements

1. Process and Procedures

Generally, requirements related to process and procedures for compliance of each specific cybersecurity levels are indicated in Table 4.1.

Table 4.1 Requirements related to process and procedures

1. Asset Management		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
– Physical devices and systems within the organization are inventoried – Software platforms and applications installed onboard of ships/offshore are to be inventoried – Onboard communication and data flows are mapped – External information systems are catalogued – Resources (e.g., hardware, devices, data and software) are prioritized based on their classification, criticality, and business value – Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established – Ownership of all software assets is to be identified. – The inventory is to be updated after any asset change. – Critical areas having sensitive information and appropriate access control measures are to be identified. – Systems, loss of which can have impact on critical nature of business undertaken by the ship, are to be identified; – Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools; – Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	In addition to Cybersecurity Level 1: – The asset registry is to be reviewed and updated with every: • change in operation area; • change of flag; • change of class; • changes in its IT or OT systems – The ship is to formulate a procedure for patch management. Patch management tasks include maintaining current knowledge of available patches, identify patches appropriate for particular systems and ensure installation of patches in accordance with manufacturer recommendations. The updated software is to be tested and the asset registry is to be updated. – Asset replacements are to be verified with base line configurations. – Following requirements are to be complied with as applicable: • Replaced assets are to be verified with base line configurations; • Asset changes are to be managed; • Assets are to be prioritized; • The asset inventory is to be current. • Firmware is to be updated as per manufacturer recommendations and updated asset is to be tested. When the asset forms a part of an integrated system, then the complete integrated system is to be tested,	In addition to Cybersecurity Level 2: – The asset registry is to include all the ship IT, OT assets and associated networks. – Asset registry is to be reviewed periodically and upon any change of asset configuration, or upgradation due to evolving technology.

Table 4.1 Requirements related to process and procedures (*continued*)

2. Governance		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
– Cybersecurity policy for the ship is established and communicated. – A business continuity plan in the event of cyber-attack on critical systems is to be approved and documented. – Operational objectives and activities are to be established, prioritized and communicated to all concerned. – Governance process is to address cyber security risks at high level. – Clear definition of roles and responsibilities with regard to cybersecurity ~~safety~~ is to be formulated. – Legal and regulatory/requirements regarding Cybersecurity are to be identified. – A suitable risk assessment approach is to be identified. – The senior management and employees working on critical cyber systems are to have general awareness on cyber safety. – Ship cyber safety officer (SCSO) is to be designated who would be responsible for implementation of cyber risk management. – Procedure for monitoring of regulatory requirements and addressing them is to be formulated.	In addition to Cybersecurity Level 1, – The policies and procedures are to be reviewed periodically and the revised approved policies are to be communicated to all concerned. The review periodicity is to be defined. – Procedures are to be established and reviewed with respect to the addition, removal and disposal of all assets. – The implemented controls are to be verified towards compliance to requirements indicated in this section. The results of verification are to be considered during review of policies and procedures.	In addition to Cybersecurity Level 2, – All the third party vendors, service providers who interact with the shi cyber systems are to be identified; – An agreement with third party insisting on implementation of basic cyber safety control such as fire walls, antivirus etc. at their end is to be formulated; Responsibilities of third party are to be clearly defined; – Responsibilities are to be clearly defined for cyber security and related physical security activities. – Specific clauses in contract with third party to manage cyber risk are to be included. Typical clauses are to include non-disclosure agreement, immediate communication on any detected risk by the third party which can affect the ship. – Position in critical infrastructure and its industry sector is to be identified; – Mission, objectives and activities are to be prioritized and established; – Dependencies on critical infrastructure and critical services are to be established; – Resilience requirements to support critical infrastructure are to be identified and communicated; – Critical information system components and functions are to be identified by performing a criticality analysis; – Knowledge of its role in the larger ecosystem, but has formalized its capabilities to interact and share information externally

Table 4.1 Requirements related to process and procedures (*continued*)

3. Risk Assessment		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
– Established risk register and acceptance criterion; – Identification and record of consequences of each threat on vulnerable system; – Approved and documented risk methodology; – Identification of risk priorities based on consequence and severity ~~of~~ impact; – Risk classification; – Identified risks which can be mitigated/accepted. – Asset vulnerabilities are identified and documented – Threats, both internal and external, are identified and documented – Potential business impacts and likelihoods are identified – Threats, vulnerabilities, likelihoods, and impacts are used to determine risk – Risk responses are identified and prioritized	In addition to Cybersecurity Level 1 – Risks indicators and threats are to be regularly reviewed and updated as necessary; – Threat and vulnerability information is received from information sharing forums and sources; – Updates the risk assessment or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. – Each cyber safety related incident is to be recorded and reviewed periodically for lessons learnt; – Methods for assess and address data integrity risks are to be formulated and implemented; – Consequences of accepted and residual risks are to be reviewed periodically; – Results of Vulnerability scans are to be performed and results are to be used in risk assessment; – A security policy is established, legal and regulatory requirements regarding cyber security are understood and managed; – Information about technical vulnerabilities of information systems being used are to be obtained in a timely fashion, the ship's exposure to such vulnerabilities is to be evaluated and appropriate measures taken to address the associated risk; – Periodic reviews of risk management process for IT and OT systems are to be carried out. The document is to define the periodicity of review.	In addition to Cybersecurity Level 2 – Risk management processes are to be established, managed and agreed ~~to~~ by stakeholders; – Goals for penetration testing are to be clearly defined and the same is to be communicated to the test team; – The network architecture is to be evaluated for an appropriate defense-indepth security strategy; – A strategy for using firewalls is to be developed and functional demilitarized zone DMZs are to be established; – Information which can be shared with test team as per the desired mode of testing i.e. black box, grey box or white box testing, is to be clearly defined.

Table 4.1 Requirements related to process and procedures (*continued*)

4. Physical & system access control		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
– The ship: • Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; • Issues authorization credentials for facility access; • Reviews the access list detailing authorized facility access by individuals • Removes individuals from the facility access list when access is no longer required. – Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. – Equipment, information or software shall not be taken off-site without prior authorization. – Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented. – Safety levels required for systems/ equipment based on risk assessment are to be identified and implemented; – The administrative controls for system log are to be implemented; – Measures to ensure Endpoint Security are to be implemented; – Removable media is to be protected and its use restricted according to policy; – Policy to limit the use of external devices e.g. USB devices is to be formulated and implemented; – Email policy measures are to be implemented; – The control system is to provide the capability to uniquely identify and authenticate all human users.. – Access accounts are to be role based to manage access to appropriate information or systems for that user's role	In addition to Cybersecurity Level 1, – Access control measures are to be reviewed periodically. Detected access breach incidents are to be considered in review. – Suitable measures are to be identified and implemented to address the Identified issues. Base line authentication procedures for remote users is to be implemented. The ship is to area specific system authorization.	In addition to Cybersecurity Level 2, – The ship is to implement advanced authentication controls. For system access. – Physical and system access can be implemented function specific or zone specific. The procedures and controls are to reviewed periodically. Information new threat, breaches are to be analysed and existing process is to be reviewed/updated as required.

Table 4.1 Requirements related to process and procedures (*continued*)

4. Physical & system access control		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
– The allocation of privileged access rights is to be restricted and controlled. – Identities and credentials are managed for authorized devices and users		
5. Network Security		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
– All networks in the ship are to be inventoried; – The ship is to have a policy to maintain network integrity – Measures to ensure perimeter security are to be implemented;	In addition to Cybersecurity Level 1 – In addition to perimeter security and creation of Demilitarised Zone (DMZs), the network security is to be augmented by provision of VPNs and VLANs. – Formal transfer policies, procedures and controls are to be in place to protect the transfer of information through the use of all types of communication facilities. – The control system is to provide the capability to deny network traffic by default and allow network traffic by exception. – Communication and control networks are to be protected	In addition to Cybersecurity Level 2 Mobile device security – Usage restrictions and implementation guidance for ship controlled portable and mobile devices are to be formulated; – Connection of mobile devices is to be authorized meeting defined usage restrictions and implementation guidance; – Monitoring for unauthorized connections of mobile devices to ship information systems is to be undertaken Wireless device security – Usage restrictions and implementation guidance for wireless access are to be established; – Unauthorized wireless access to the information system is to be monitored; – Wireless access to the information system prior to connection is to be authorized. Network segmentation – Division of large networks into separate network domains (segments); – Consideration of physical and logical segregation; – Definition of domain perimeters; – Definition of traffic rules between domains; – Usage of authentication, encryption, and user-level network access control technologies

Table 4.1 Requirements related to process and procedures (*continued*)

6. System Security Controls		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
– Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools – Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access – Assets are formally managed throughout removal, transfers, and disposition Adequate capacity to ensure availability is maintained	In addition to Cybersecurity Level 1 Data Security – Policies and procedures for management of information data in accordance with its defined risk strategy are to be developed; – Protections against data leaks are formalized and implemented – Back-up procedures for critical data are to be identified; – Protection for data-at-rest and data-in-transit is to be implemented – The control system is to provide the capability to protect integrity of sessions and is to reject any usage of invalid session IDs; – Integrity checking mechanisms are used to verify software, firmware, and information integrity – Detection, prevention and recovery controls to protect against malware are to be implemented. Information protection – A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) – Configuration change control process is to be established; – Systems backup are to be taken at clearly defined back up period. Procedure for testing the backs ups is to be established; – Policy and regulations regarding the physical operating environment for ships assets are met – A process to continually improve the protection process is to be available; – Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are to be established	In addition to Cybersecurity Level 2 – The development and testing environment(s) are separate from the production environment Integrity checking mechanisms are used to verify hardware integrity

Table 4.1 Requirements related to process and procedures (*continued*)

6. System Security Controls		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
	– Procedures and processes for testing response and recovery plans are to be available; – Cybersecurity is to be included in human resources practices (e.g., deprovisioning, personnel screening) – A vulnerability management plan is developed and implemented	

7. Detection Procedures		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
– Roles and responsibilities for detection are well defined to ensure accountability – Detection activities comply with all applicable requirements – Detection processes are tested – Event detection information is communicated – Detection processes are continuously improved – Barriers to prevent unauthorized access into critical systems; – The ship is to formulate a policy on removable media; – Intrusion preventions systems (fire walls etc.); – Procedures for accessing systems; – Controls implemented for the systems (IT and OT) are to be suitable. – A baseline configuration of information technology/control systems is created and maintained	In addition to Cybersecurity Level 1, – A baseline of network operations and expected data flows for users and systems is established and managed – Procedures and controls are to be defined and implemented to detect and analyze anomalous activities in timely manner; – Potential impacts of detected anomalies are to be identified; – All IT and OT systems are to be monitored at regular intervals for unusual activities and breaches; – Procedures for communication and immediate action when an anomaly is detected are to be formulated; – Implementation of detection process such as fire walls, intrusion detection and prevention systems to identify threats; – Periodically evaluate overall security management system to ensure the security objectives are met and detection processes are continuously improved; – Investigation of notifications from detection systems is to be undertaken – Detected events are analyzed to understand attack targets and methods Event monitoring – the detection process is to be regularly updated and tested in line with latest technology;	In addition to Cybersecurity Level 2, – The system is to have the capability to protect the confidentiality of information at rest, during remote access sessions and during traversing of an untrusted network is to be provided. Encryption is a common mechanism for ensuring information confidentiality.

Table 4.1 Requirements related to process and procedures (*continued*)

7. Detection Procedures		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
–	– procedures are to be in place to assess the requirements of detection process when any new system is added/ replaced; – Process for various types of detection methods based on criticality and vulnerability of the systems are identified by the ship; – Incident thresholds are to be established. – Event data are aggregated and correlated from multiple sources and sensors – Impact of events is determined – The network is monitored to detect potential cyber security events – Monitoring for network and personnel activity in general are to be carried out at centralized station – Monitoring for unauthorized personnel, connections, devices, and software is performed.	
8. Training, Awareness and Information Sharing		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
– Key senior personnel who would be involved in top level decisions towards cyber safety implementation are to be identified and communicated; – Cyber safety training needs relevant to the job are to be identified; – All users are informed and trained – Privileged users understand their roles and responsibilities – Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities – Senior executives understand their roles and responsibilities – Physical and cybersecurity personnel understand their roles and responsibilities	In addition to Cybersecurity Level 1 – Process to update its senior management on impact of cyber risks on legal and business aspects are to be defined; – A formal process to identify the training by the line manager is to be in place; – Provision is to be made for subject matter external experts for training; – Training requirements, that address internal threats, lessons learnt and external cyber information are to be defined; – Specific programs to train its employees on Operation technology and Information technology are to be established;	In addition to Cybersecurity Level 2 – The ship is to have a procedure for receipt of information that enables collaboration and risk-based management decisions in response to events is to be ensured; Information is to be actively shared to ensure that accurate, current information is distributed and consumed to improve cyber safety before a cybersecurity event occurs

Table 4.1 Requirements related to process and procedures (*continued*)

8. Training, Awareness and Information Sharing		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
	– Effective communication of updated information on cyber safety is made to its employees through various communication media. For e.g. Emails, seminars, workshops, etc. – Procedures to implement preventive maintenance routines such as anti-virus and anti-malware, patching, backups, and incidence-response planning and testing are to be covered as part of training.	
9. Response and Recovery Procedures		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
– Methods are to be established and documented for responding to an incident; – Persons responsible for incident response and back-up are to be clearly identified and their roles defined; – Each incident is to be recorded and reviewed periodically for lessons learnt – Location of software and hardware required for backups are to be documented and inventoried; – Location of back-up storage, authorization for retrieval for backups are to be defined and documented; – A back-up policy in the event of cyber system being compromised is to be documented along with procedures for implementation. The document is also to indicate the roles and responsibilities of persons involved; – The information security issues in the development, documentation, an updating of a critical infrastructure and key resources protection plan are to be addressed; – Personnel are to know their roles and order of operations when a response is needed – Events are to be reported consistent with established criteria; – Recovery plan is to be executed during or after an event.	In addition to Cybersecurity Level 1: – The ship is to have Cyber Safety Response Team (CSRT) to deal with all types of cyber threats; – The rules and responsibilities of the CSRT are to be clearly defined; – The ship is to have procedures and methods to regularly monitor and update its response plans; – Process for early warning system and means to communicate are to be clearly defined. – Notifications from detection systems are investigated Communication – All the internal stake holders who need to be communicated with, in an emergency, are to be identified; – Ways of communications for internal stake holders are to be clearly defined; – Information required to be communicated to every person is to be clearly defined; – All the external stake holders who are required to be communicated in emergency are to be identified; – Mode of communication to external stakeholders is to be defined; – Extent of information which needs to be communicated is to be defined;	In addition to Cybersecurity Level 2: – Coordination with stakeholders is to be carried out in accordance with established response plans; – A disaster recovery plan is to be formulated, approved and tested periodically. The personnel involved identified in disaster recovery plan are to be communicated about their roles and responsibilities in the event of disaster.

Table 4.1 Requirements related to process and procedures (*continued*)

9. Response and Recovery Procedures		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
Communication – Personnel know their roles and order of operations when a response is needed; – Incidents are reported consistent with established criteria; – Information is shared consistent with response plans; – Coordination with stakeholders occurs consistent with response plans; – Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness; – Public relations are managed; – Reputation is repaired after an incident; – Recovery activities are communicated to internal and external stakeholders as well as executive and management teams; Analysis – Notifications from detection systems are investigated – The impact of the incident is understood – Forensics are performed – Incidents are categorized consistent with response plans – Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	– Any specific authorization required before communicating sensitive information is to be established; – Communication to media is to be defined i.e. what to communicate and who would communicate; – Redundant communication paths, in the event of loss of primary communication path are to be identified. Recovery management – The ship has to formulate and document a well-defined recovery and back up procedures; – Critical systems and data which need to be recovered in the event of cyber-attack are to be identified; – Location of back up storage, authorization for retrieval for backups are to be defined and documented; – Personnel, teams who are responsible for recovery are to be identified; – Procedures are to be formulated to train personnel in backup and recovery process; – Procedures for dealing with the loss or theft of unencrypted backup tapes that contain proprietary or sensitive information are to be formulated; – The ship has a documented emergency plan in place.	

Table 4.1 Requirements related to process and procedures (*continued*)

9. Response and Recovery Procedures		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
Mitigation – Incidents are contained – Incidents are mitigated – Newly identified vulnerabilities are mitigated or documented as accepted risks Improvement – Response plans incorporate lessons learned – Response strategies are updated		
10. Cyber safety process review		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
– Review of the risk assessment and mitigation controls is to be carried out upon any addition of new asset or change in model /make of asset of the risk assessment and mitigation controls is to be carried out upon any addition of new asset or change in model /make of asset. – The revised policies and procedures are to be approved.	In addition to Cybersecurity Level 1: – The cyber safety technical controls and procedures are to be reviewed periodically. The periodicity level is to be defined, – The threat information results received from the analysis of detected threats, is to be considered in the review process. – Threat information from similar industries received from various forums is to be considered in risk analysis.	In addition to Cybersecurity Level 2: Continual improvement. Following requirements as applicable are to be complied with: – A current profile of ships' cyber risk practices is prepared and the extent to which it has progressed in implementation of cyber safety practices to meet the five functional requirements specified in cyber safety philosophy: Identify, Protect, Detect, Respond, and Recover, is to be carried out; – Review its policies and procedures with respect to changes in international/ national scenarios; – Use the above information to reprioritize resources to strengthen other cyber safety practices; – Incorporate the lessons learnt and best practices from industry; – Consistently exhibit commitment towards cyber safety through repeated successful audits, so that cyber safety becomes an organizational culture; – Cater for capital planning by way of budget allocation for cyber safety; – A system to receive threat and vulnerability information from information sharing forums and sources is implemented; – Compare the current profile and the target profile to determine gaps;

Table 4.1 Requirements related to process and procedures (*continued*)

10. Cyber safety process review		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
		– Continuously review and improve the existing process, procedures, effectiveness, information /data security management systems; – Procedures are to be established and audited with respect to the addition, removal and disposal of all assets; – Event detection information is to be communicated to appropriate parties; – Voluntary information sharing is to occur with external stakeholders to achieve broader cybersecurity situational awareness.

2. Requirements for Information Technology (IT)

Requirements related to Information Technology (IT) for compliance of cyber security notations are indicated in Table 4.2.

Table 4.2 Requirements related to IT systems

1. Asset Management		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
– All ship's IT systems required for intended operations are to be identified and documented. – Assets associated with information and information processing facilities are to be identified and inventoried. – Formal transfer policies, procedures and controls are to be in place to protect the transfer of information through the use of all types of communication facilities. – Information is to be classified in terms of value, criticality and sensitivity to unauthorised disclosure or modification. – Vulnerabilities in information systems required for intended operations of the vessel are to be identified.	Requirements in Cybersecurity Level 1 also applied.	Requirements in Cybersecurity Level 2 also applied.

Table 4.2 Requirements related to IT systems(*continued*)

2. Governance		
Cybersecurity Level 1	Cybersecurity Level 2	Cybersecurity Level 3
– A set of policies for information security are to be defined, approved by management, documented and communicated to employees and relevant personnel. – All information security responsibilities are to be defined and allocated. – A contingency plan is to be developed for the information system which identifies – essential missions and business functions and associated contingency requirements. – Provides recovery objectives, restoration priorities, and metrics. – Addresses contingency roles, responsibilities. – Where required a person on board is to be identified to assist ship cyber security officer on information system. – The selected risk assessment and analysis approach and methodology is to identify and prioritize risks based upon security threats, vulnerabilities and consequences related to their information systems.	Requirements in Cybersecurity level 1 also applied.	In addition to Cybersecurity level 1, – Cyber security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) towards information systems are to be established. – All information security responsibilities are to be defined and allocated to third party stake holders – All information security responsibilities are to be defined and allocated. – Patch updating process with third party software providers is to be formulated – Management is to require all employees and contractors to apply information security in accordance with the established policies
3. Risk Assessment		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– The ship: • Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; • Documents risk assessment results in risk assessment report; • Reviews risk assessment results defined frequency	In addition to Cybersecurity level 1, – Vulnerability tests are to be conducted from external to ship network and internal ship network zones. – Appropriate contacts with special interest groups or other specialist security forums and professional associations be maintained.	In addition to Cybersecurity level 2, – Determination of risk tolerance for information systems is decided by its role in critical infrastructure and sector specific risk analysis – Knowledge gained from analysing and resolving information security incidents is to be used to reduce the likelihood or impact of future incidents. Penetration testing is carried out at defined frequency on identified information systems or system components;

Table 4.2 Requirements related to IT systems (*continued*)

3. Risk Assessment		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– The ship: • Develops a comprehensive strategy to manage risk to ship operations and assets, individuals associated with the operation and use of information systems; • Implements the risk management strategy consistently; • Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information – Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. – A formal user registration and deregistration process shall be implemented to enable assignment of access rights. Create, enable, modify, disables, and remove information system accounts in accordance with defined procedures or conditions; – Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification		– Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; – Documents risk assessment results in risk assessment report – Reviews risk assessment results at defined frequency
4. Physical & System access control		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information – Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Requirements in Cybersecurity level 1 also applied.	Requirements in Cybersecurity level 1 also applied.

Table 4.2 Requirements related to IT systems (*continued*)

4. Physical & System access control		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. – A formal user registration and deregistration process shall be implemented to enable assignment of access rights. Create, enable, modify, disables, and remove information system accounts in accordance with defined procedures or conditions; – Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification		
5. Network Security		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– All networks serving Information systems are to be inventoried – Networks shall be managed and controlled to protect information in systems and applications	In addition to Cybersecurity level 1, – The allocation and use of privileged access rights is to be restricted and controlled – Users are to be provided with access to the information system network and network services that they have been specifically authorized to use. – The control system is to provide the capability to protect the integrity of sessions. The control system is to reject any usage of invalid session IDs	In addition to Cybersecurity level 2, Mobile device security – Procedures be implemented to control the installation of software on operational systems. – Defines acceptable and unacceptable mobile code and mobile code technologies; – Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and – Authorizes, monitors, and controls the use of mobile code within the information system. Wireless device security – Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and – Authorizes wireless access to the information system prior to allowing such connections Network segmentation – Procedures for authentication, encryption, and user-level network access control technologies are to be implemented

Table 4.2 Requirements related to IT systems (*continued*)

6. System Security Controls		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. – Equipment, information or software shall not be taken off-site without prior authorization. – Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	In addition to Cybersecurity level 1, **Data security** – Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. – Procedures for handling assets are to be developed and implemented in accordance with the information classification scheme adopted by the ship – Networks are to be managed and controlled to protect information in systems and applications. – Formal transfer policies, procedures and controls is to be in place to protect the transfer of information through the use of all types. – Information involved in electronic messaging is to be appropriately protected. – Information involved in application service transactions is to be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. Backup copies of information, software and system images are to be taken and tested regularly in accordance with an agreed backup policy. – Conflicting duties and areas of responsibility is to be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the Ship's assets. – Users are to be provided with access to the network and network services that they have been specifically authorized to use. – An access control policy is to be established, documented and reviewed based on business and information security requirements. – The allocation and use of privileged access rights are to be restricted and controlled. Procedures are to be implemented to control the installation of software on operational systems	In addition to Cybersecurity level 2,

Table 4.2 Requirements related to IT systems (*continued*)

6. System Security Controls		
– Cybersecurity level 1	– Cybersecurity level 2	Cybersecurity level 3
	– Groups of information services, users and information systems is to be segregated on networks. Information protection – Changes to, business processes, information processing facilities and systems that affect information security is to be controlled. Rules governing the installation of software by users are to be established and implemented – When operating platforms are changed, business critical applications are to be reviewed and tested to ensure there is no adverse impact on operations or security. – Backup copies of information, software and system images is to be taken and tested regularly in accordance with an agreed backup policy. – The Ship is to establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation. – Equipment is to be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. – Procedures for handling assets are to be developed and implemented in accordance with the information classification scheme adopted by the Ship. – Procedures are to be implemented for the management of removable media in accordance with the classification scheme adopted by the Ship – The use of utility programs that might be capable of overriding system and application controls is to be restricted and controlled –	

Table 4.2 Requirements related to IT systems (*continued*)

6. System Security Controls		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
	– The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on defined information flow control policies.	
7. Detection Procedures		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– Barriers to prevent unauthorized access into critical systems is to be implemented; – The ship is to formulate a policy on removable media; – Intrusion preventions systems (fire walls etc.) is to be implemented; – Procedures for accessing systems is to be established and implemented; – Controls implemented for the systems (IT and OT) are to be suitable. A baseline configuration of information technology/control systems is created and maintained	In addition to Cybersecurity level 1, – The ship is to establish a list of triggers with set thresholds, which would result in a review of related elements of the Control system management. These triggers include at a minimum: occurrence of serious security incidents, legal and regulatory changes, – Changes in risk and major changes to the Control system. The thresholds should be based on the defined risk tolerance. – Management responsibilities and procedures are to be established to ensure a quick, effective and orderly response to information security incidents. Event monitoring – Information security events are to be Assessed Cyber safety centre – Information about technical vulnerabilities of information systems being used is to be obtained in a timely fashion, the Ship's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk – Event logs recording user activities, exceptions, faults and information security events are to be produced, kept and regularly reviewed. The Ship develops a continuous monitoring strategy and implements a continuous monitoring program that includes: • Establishment of defined metrics to be monitored as per defined frequency • Ongoing security control assessments in accordance with the Ship continuous monitoring strategy;	Requirement in Cybersecurity level 2 also applied

Table 4.2 Requirements related to IT systems (*continued*)

7. Detection Procedures		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
	• Ongoing security status monitoring of Ship-defined metrics in accordance with the continuous monitoring strategy; • Correlation and analysis of security related information generated by assessments and monitoring; • Response actions to address results of the analysis of security-related information; and • Reporting the security status to defined personnel	
8. Training, Awareness and Information Sharing		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– All personnel using information systems shall be trained initially and periodically thereafter in the correct security procedures and the correct use of information processing facilities – All information security responsibilities shall be defined and allocated.	In addition to Cybersecurity level 1, – Provision for training the ship staff by the IT system manufacturer is to be implemented. The effectiveness of training is to be ascertained.	In addition to Cybersecurity level 2, – Information security events is to be reported through appropriate management channels as quickly as possible. – Knowledge gained from analysing and resolving information security incidents is to be used to reduce the likelihood or impact of future incident and is to be shared. – Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information – Employs defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions. – Voluntary information sharing is to occur with external stakeholders to achieve broader cybersecurity situational awareness.
9. Response and Recovery Procedures		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– All information security responsibilities shall be defined and allocated – Appropriate contacts with relevant authorities shall be maintained – Information security events shall be reported through appropriate management channels as quickly as possible.	In addition to Cybersecurity level 1, – Appropriate contacts with relevant authorities shall be maintained – Information security incidents are to be responded to in accordance with the documented procedures – The Ship establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.	Requirement in Cybersecurity level 2 also applied

Table 4.2 Requirements related to IT systems (*continued*)

9. Response and Recovery Procedures		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– The ship Develops a contingency plan for the information system that: • Identifies essential missions and business functions and associated contingency requirements; • Provides recovery objectives, restoration priorities, and parameters. • Addresses contingency roles, responsibilities, assigned individuals personnel with contact information; • Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure • Is approved by authorised personnel – Organization shall define the frequency to review the contingency plan for the information system. – Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; – Protects the contingency plan from unauthorized disclosure and modification	– Knowledge gained from analysing and resolving information security incidents are to be used to reduce the likelihood or impact of future incidents (lesson to be learnt) – Event logs recording user activities, exceptions, faults and information security events are to be produced, kept and regularly reviewed. – Information security events are to be assessed	
10. Cyber safety process review		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
		– Protects the contingency plan from unauthorized disclosure and modification – Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; – Coordinates incident handling activities with contingency planning activities; – Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

Table 4.2 Requirements related to IT systems (*continued*)

10. Cyber safety process review		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
		– Formulate procedures for employee personnel data management, in addition to informational data security; – Data System is to be designed with adequate capacity; – Develop a policy addressing remote login by a user and/ or remote connections. Additional controls to automatically terminate remote access may be implemented as per the asset desired security level – The cyber-attack detection methods for information system are to be periodically tested and continuously improved – A system to receive threat and vulnerability information for the information system from information sharing forums and sources and manufacturer is implemented;

3. Requirements for Operational Technology (OT)

Requirements related to Operational Technology (OT) for compliance of cyber security notations are indicated in Table 4.3.

Industrial standard (e.g., IEC 62443, NIST Special Publication 800-82r2) are to be referenced for technical detail as required, as appropriate for the arrangement utilized. An assessment version of the OT specification, mapped to applicable industry standards (i.e., IEC 62443 and NIST Cybersecurity Framework), is to be available separately as an additional resource for OT security, to be provided as a Guidance Note for self-assessment or survey.

Table 4.3 Requirements related to OT systems

1. Asset Management		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– All control systems required for vessel propulsion, safety and navigation systems including systems to effectively carry out the intended operation of the vessel are to be inventoried. – The ship is to identify the various control systems, gather data about the devices to characterize the nature of the security risk. The controls systems and group the devices into logical systems. (Propulsion, navigation etc.)	Requirements in Cybersecurity level 1 also applied.	Requirements in Cybersecurity level 2 also applied.

Table 4.3 Requirements related to OT systems (*continued*)

1. Asset Management		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– Control systems software including their version numbers used for vessel propulsion, safety and navigation systems including systems to effectively carry out the intended operation of the vessel are to be inventoried. – The control systems are to be prioritised based on their criticality to perform vessel functions. A priority rating may be assigned towards mitigation of risks. – A detailed vulnerability assessment of all individual cyber controlled control systems is to be carried out. – The organization approves, controls, and monitors information system maintenance tools		
2. Governance		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– A high-level system risk assessment is to be performed to understand the safety, operational, environmental in the event that availability, integrity or confidentiality of the ship control system is compromised. – The personnel responsible for various ship control systems are to be clearly identified and their responsibilities are to be defined. – The selected risk assessment and analysis approach and methodology is to identify and prioritize risks based upon security threats, vulnerabilities and consequences related to their systems – The results of physical, HSE and cybersecurity risk assessments are to be integrated to understand the assets' overall risk. – All personnel that perform risk management, control system engineering, system administration/ maintenance and other tasks related to control system management are to be trained on the security objectives and operations for these tasks.	Requirements in Cybersecurity level 1 also applied.	In addition to Cybersecurity level 2 – Cyber security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) towards ship control systems are to be established. – All personnel (including employees, contract employees, and third party contractors) are to be trained initially and periodically thereafter in the correct security procedures and the correct use of Control systems.

Table 4.3 Requirements related to OT systems (*continued*)

2. Governance		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– A contingency plan for the critical control systems is to be developed. The plan is to identify control systems required for essential operations of the vessel and evolve contingencies. – The contingency plan is to identify restoration objectives and priorities for restoration. – Where required a person is to be identified to assist the ship cyber safety officer in cyber safety issues.	Requirements in Cybersecurity level 1 also applied.	In addition to Cybersecurity level 1 – Cyber security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) towards ship control systems are to be established. – All personnel (including employees, contract employees, and third party contractors) are to be trained initially and periodically thereafter in the correct security procedures and the correct use of Control systems.
3. Risk Assessment		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– The risk assessment methodology is to include methods for prioritizing detailed vulnerabilities identified in the detailed vulnerability assessment. – Control system cyber risks that ship faces are identified and the likelihood and severity of these risks are assessed – A detailed risk assessment is to be carried out. – Risk assessments shall be conducted through all stages of the technology lifecycle including development, implementation, changes and retirement (for new construction) – Reduce risk to and maintain risk at an acceptable level in the CONTROL SYTEM based upon the ship's tolerance for risk. – The ship shall determine and document its risk tolerance as a basis for creation of policy and risk management activities.	In addition to Cybersecurity level 1 – Vulnerability tests are to be conducted for internal ship control system network zones and also from external network when control system has provision for remote connection. – A Set of control system cyber risks are to be identified that ship faces and assess the likelihood and severity of these risks. – The Ship is to conduct a detailed risk assessment incorporating the vulnerabilities identified in the detailed vulnerability assessment. – Risk assessments are to be conducted through all stages of the technology lifecycle including development, implementation, changes and retirement.	In addition to Cybersecurity level 2 – Identify the set of Control system (CS) cyber risks that a ship faces and assess the likelihood and severity of these risks. – determination of risk tolerance for control systems is decided by its role in critical infrastructure and sector specific risk analysis – A detailed risk assessment incorporating the vulnerabilities identified in the detailed vulnerability assessment is to be conducted. – Risk assessments is to be conducted through all stages of the technology lifecycle including development, implementation, changes and retirement. – Penetration testing for control systems networks is to be carried out as per control system manufacturer recommendations. The testing is recommended to be carried out when the vessel is idling at harbour.
4. Physical & System access control		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– One or more physical security perimeters shall be established to provide barriers to unauthorized access to protected assets. – Procedures shall be established for monitoring and alarming when physical or environmental security is compromised.	Requirements in Cybersecurity level 1 also applied.	Requirements in Cybersecurity level 1 also applied.

Table 4.3 Requirements related to OT systems (*continued*)

4. Physical & System access control		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– Access privileges implemented for access accounts shall be established in accordance with the defined authorization security policy – Any remote login to the control system is to be controlled and is to be authorised by SCSO – Access accounts should be role based to manage access to appropriate information or systems for that user's role. Safety implications shall be considered when defining roles.		
5. Network Security		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– All networks serving ship's control system either in standalone mode (sensor to server network) and/or interconnected systems are to be inventoried The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.	In addition to Cybersecurity level 1, – The allocation and use of privileged access rights is to be restricted and controlled – Users are to be provided with access to the control system network and network services that they have been specifically authorized to use (principle of least privilege). – The control system is to provide the capability to protect the integrity of transmitted information – The control system is to provide the capability to protect the integrity of sessions. The control system is to reject any usage of invalid session IDs Group and separate key cybersecurity devices into zones with common security levels in order to manage security risks and to achieve a desired target security level for each zone.	In addition to Cybersecurity level 2, Mobile device security – The control system is to provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the control system that include: • preventing the execution of mobile code; • requiring proper authentication and authorization for origin of the code; • restricting mobile code transfer to/from the control system; and • monitoring the use of mobile code. Wireless device security – The control system is to provide the capability to identify and authenticate all users (Personnel, software processes or devices) engaged in wireless communication. – The control system is to provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices. Network segmentation – The control system is to provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

Table 4.3 Requirements related to OT systems (*continued*)

6. System Security Controls		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– Using clearly defined criteria, proposed changes to Control system shall be reviewed for their potential impact to HSE risks and cyber security risks by individuals having necessary technical knowledge about the operation and the Control systems. – The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. – All equipment assets, including auxiliary environmental equipment, shall be properly maintained to ensure proper operation. – Information system maintenance tools is approved, controlled and monitored – Detection and prevention controls to protect against malware at server and end user level;	In addition to Cybersecurity level 1 Data Security – The control system is to provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit. – The control system is to provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned. – The control system is to provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest – The control system is to provide the capability to employ cryptographic mechanisms to recognize changes to information during communication – The control system is to provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception) – The control system is to provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during operation and or scheduled maintenance. Information protection – A change management system for the CS environment is to be developed and implemented – Ship is to follow separation of duty principles to avoid conflicts of interest. – The control system is to provide the capability to prevent unauthorized and unintended information transfer via volatile shared memory resources. – Security policies and procedures that address both physical and cyber security in the protection of assets are to be established.	Requirements in Cybersecurity level 2 also applied

Table 4.3 Requirements related to OT systems (*continued*)

6. System Security Controls		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
	– The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) is to be supported by the control system without affecting normal plant operations. – The control system is to provide the capability to recover and reconstitute to a known secure state after a disruption or failure. – A procedure for backing up and restoring computer systems and protecting backup copies is to be established, used, and verified by appropriate testing. – The control system is to provide the capability to be configured according to recommended network and security configurations. – The control system is to provide an interface to the currently deployed network and security configuration settings. – The control system is to provide the capability to employ cryptographic mechanisms to recognize changes to information during communication. – On all interfaces, the control system is to provide the capability to enforce authorizations assigned to all users (humans, software processes and devices) for controlling use of the control system to support segregation of duties and least privilege	
7. Detection Procedures		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– Using clearly defined criteria, proposed changes to control system shall be reviewed for their potential impact to HSE risks and cyber security risks by individuals having necessary technical knowledge about the operation and the Control systems. – The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier.	In addition to Cybersecurity level 1, – The control system is to provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance – Individual audit records is to include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.	Requirements in Cybersecurity level 2 also applied

Table 4.3 Requirements related to OT systems (*continued*)

7. Detection Procedures		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– The control system shall provide an interface to the currently deployed network and security configuration settings. – A change management system for the Control system environment shall be developed and implemented. The change management process shall follow separation of duty principles to avoid conflicts of interest.	– The control system allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management (e.g. NIST 800-92) and system configuration. – The control system is to provide the capability for authorized humans and/or tools to access audit logs on a read-only basis. – The detail of an identified incident is to be documented to record the incident, the response, the lessons learned, and any actions taken to modify the control system management system in light of this incident. Event monitoring – The Ship is to identify the risk and vulnerability reassessment frequency as well as any reassessment triggering criteria based on technology, Ship, or industrial operation changes. Cyber safety center – The control system is to provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.	
8. Training, Awareness and Information Sharing		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– All personnel that perform risk management, control systems engineering, system administration/maintenance and other tasks that impact the control system management system are to be trained on the security objectives and industrial operations for these tasks.	In addition to Cybersecurity level 1, – The Ship is to provide role-based security training to personnel with assigned security roles and responsibilities: – Training on control systems is to be carried out Before authorizing access to the system or performing assigned duties or when required by system changes – The ship shall have program to train its personnel on recent developments on control and automation systems. – Provision for training the ship staff by the control system manufacturer is to be implemented. The effectiveness of training is to be ascertained.	In addition to Cybersecurity level 2, – The control system is to provide the capability for authorized humans and/or tools to access audit logs on a read-only basis. – The ship implements a Control systems threat awareness program that includes a cross-organization information sharing capability. – Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.

Table 4.3 Requirements related to OT systems (*continued*)

9. Response and Recovery Procedures		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
– The incident response plan shall be communicated to all appropriate organizations – The organization should establish a reporting procedure to communicate unusual activities and events that may actually be cyber security incidents – The organization should report cyber security incidents in a timely manner (ASAP) – The details of an identified incident shall be documented to record the incident, the response, the lessons learned, and any actions taken to modify the Control System Management System (CSMS) in light of this incident.	In addition to Cybersecurity level 1 – The Ship is to implement an incident response plan that identifies responsible personnel and defines actions to be performed by designated individuals – If an incident is identified, the Ship is to promptly respond in accordance with the established procedures – The Ship should have procedures in place to identify failed and successful cyber security breaches	Requirement in Cybersecurity level 2 also applied
10. Cyber safety process review		
Cybersecurity level 1	Cybersecurity level 2	Cybersecurity level 3
		– The details of an identified incident is to be documented to record the incident, the response, the lessons learned, and any actions taken to modify the control system management system (CSMS) in light of this incident. The ship should establish a list of triggers with set thresholds, which would result in a review of related elements of the CSMS These triggers include at a minimum: occurrence of serious security incidents, legal and regulatory changes, changes in risk and major changes to the CS. The thresholds should be based on the ship’s risk tolerance. – Develop a policy addressing remote login by a user and/ or remote connections. Additional controls to automatically terminate remote access may be implemented as per the asset desired security level. – The cyber-attack detection methods for control system are to be periodically tested and continuously improved. – A system to receive threat and vulnerability information for the control system from information sharing forums and sources and manufacturer is implemented;

4. Requirements for Risk Assessment

4.1 Philosophy

Risk is the interplay among potential threats, Company assets, system vulnerabilities, impacts of incidents, and consequences of those incidents. The Guidelines encourages understanding of risk conditions as part of the Informed level, and as the Company expands and matures its cybersecurity program, this effort becomes risk management in the Advanced level.

A risk-based approach to cybersecurity entails the understanding of risk factors or risk conditions, with the business or mission-based grasp of assets under risk. This allows prioritization of risk mitigation efforts, and it will guide the Company in building its security capabilities, implementing its security measures, and monitoring its security systems.

The Company must understand the value of its data and its intellectual property, and the value of its functional capabilities as enabled by cyber-physical systems. If control systems did not function correctly, and production machinery or processes ceased, the effect on the Company may be strong, no matter the source of the interference or interruption. Thus, system function is considered an asset when working with control systems and operational technologies, especially in conjunction with cyber-enabled, safety-critical systems.

Assets may also include positive incentives as motivation for building capabilities, managing risks, and handling security. Data held in certain regulatory regimes, such as protected health information (PHI) or personally identifiable information (PII), or third-party data held by the Company, necessarily help the Company develop the prioritization of protections, tools and personnel assigned to protect those assets with Company systems. The Company's cybersecurity strategy, when based on risk assessment and risk understanding, will guide resource allocation in prioritization of tasks and capability development. When the most significant risk conditions or threat factors are used to develop and implement priority security controls, the Company is using a risk-based approach that can be measured and monitored.

The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of risk assessment policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure.

4.2 Cybersecurity Level 1 – Informed Cybersecurity

The requirements to be complied cybersecurity level 1 are indicated in this part.

4.2.1 Risk Management Process and Process Documentation

The Company's risk management practices are approved by internal management, but those practices are not communicated in a formal IT and/or OT cybersecurity policy document. The Company's prioritization of cybersecurity activities is evidenced by informed employees who are in turn authorized and responsible for stating and managing documented organizational risk objectives, general and industry-specific threat environments, business/mission cybersecurity requirements, and cybersecurity regulatory imperatives.

4.2.2 Formal Risk Management Program

The Company documents and demonstrates an operational/organizational commitment to IT and/or OT cybersecurity within the Company. Risk-informed, management-approved ad hoc processes and procedures are defined and implemented, and staff has adequate resources to perform IT and/or OT cybersecurity duties. However, adherence to a documented cybersecurity reference model or framework is not evident. Cybersecurity information is informally shared within the Company.

4.2.3 External Participation

The Company can articulate its role in supporting or maintaining its' role in the maritime ecosystem, but has not formalized or documented its intention or capability for interacting with and sharing IT and/or OT cybersecurity information externally.

4.3. Cybersecurity Level 2 - Advanced Cybersecurity

The requirements to be complied cybersecurity level 2 are indicated in this part. These are to be complied with, in addition to the requirements of **Cybersecurity Level 1**.

4.3.1 Risk Management Process and Process Documentation

The Company's IT and/or OT risk management practices are formally approved and expressed as policies and procedures. OT cybersecurity practices are regularly updated based on the application of risk management processes, changes in business/mission requirements, and changes to the threat and technology landscape.

4.3.2 Formal Integrated Risk Management Program

The Company demonstrates and documents an organization-wide approach to managing IT and/or OT cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, internally verified, and routinely reviewed. Formal organizations and consistent, repeatable methods are in place to respond effectively to changes in risk. Cybersecurity risk management

activities are documented for review by internal and external assessment organizations. Cybersecurity activities are resourced, and responsible personnel possess the knowledge and skills to perform their appointed IT and/or OT protection roles and responsibilities.

4.3.3 External Participation

The Company understands its dependency upon informed agencies and partners, and receives information from these agencies and partners that enables collaboration and informed risk-based management decisions within the Company to respond to OT cybersecurity events.

4.4. Cybersecurity Level 3 – Adaptive Cybersecurity

The requirements to be complied cybersecurity level 3 are indicated in this part. These are to be complied with, in addition to the requirements of **Cybersecurity Level 2**.

4.4.1 Risk Management Process and Process Documentation

The Company adapts its IT and/or OT cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the Company actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.

4.4.2 Formal Integrated Risk Management Program

There is a Company-wide approach to managing cybersecurity risk that uses formal documented risk-informed policies, processes, and procedures to address potential cybersecurity events. Formal OT cybersecurity risk management organizational functions and general organizational awareness are demonstrably part of the organizational culture as derived from an awareness of embedded activities, information shared by other sources, and continuous awareness of activities on the Company's internal and linked systems and networks.

4.4.3 External Participation

The Company maintains internal expertise on IT and/or OT cybersecurity concerns, manages risks based on cybersecurity data and acquired intelligence, and actively shares information with partners to confirm that accurate, current information is being distributed and consumed to improve cybersecurity before an IT and/or OT cybersecurity event occurs.

Section 5 Surveys and Maintenance of Class

A. General

This section provides requirement for Class Survey due to Cybersecurity notation. These surveys are generally harmonized with survey for maintain class.

B. Survey for Cybersecurity Notation

1. Survey period

All Annual and Special Periodical Surveys related with the Cybersecurity notation are to be carried out at the same time and interval as the periodical classification survey of the vessel or facility in order that they are recorded with the same crediting date.

Maintenance and calibration records are to be kept and made available for review by the attending Surveyor. The maintenance records will be reviewed to establish the scope and content of the required Annual and Special Periodical Surveys that are to be carried out by a Surveyor. During the service life of the software system components, maintenance records are to be updated on a continuing basis.

1.1 Occasional Survey

The Company is to inform BKI whenever major changes occur in any safety-critical or mission critical software systems (i.e., Category III, see Section 2.B.5.2), including systems, components or modules modified or installed in the automated and cyber-enabled systems with Cybersecurity notation. BKI may audit the vessel upon notification of an Category III system modification or installation.

2. Periodical Survey

2.1 Annual Survey

At each Annual Survey, the Surveyor is to perform an integrated software and hardware configuration audit to include verification of the following:

1) Check of asset records against Functional Specification Document (FSD) to verify accuracy of asset management efforts.
2) Change control procedures include periodic audits to confirm that procedures are also being followed.
3) Examination of Control Equipment Registry in FSD
4) Examination of Software Registry in FSD
5) Review of all control system Hardware Registry entries
6) Review records of virus and malicious software scans, and perimeter protective device logs of any events of specific interest.
7) Review records of cyber-enabled system incidents and the attendant incident response efforts, including service restoration and post-event analyses.

2.1.1 Examination of Control Equipment Registry

1) Identify control equipment that has been changed since the last audit.
2) Record each changed equipment item.
3) List all software hosted on the changed equipment.
4) Identify all documentation impacted by the change.
5) Record each documentation change.
6) Note any changes identified that were not listed on the registry.

2.1.2 Examination of Software Registry

1) Identify all control software that has been changed since the last audit.
2) Record each software item change.
3) Inspect all software hosted on the changed equipment identified in step 2.1.1.
4) Record software changes on changed equipment in the Software Registry.
5) Identify all documentation impacted by the changes.
6) Record all changed documentation in the software registry.
7) Note any software changes identified that were not listed on the registry.

2.1.3 Review of Integrated Control System's Hardware Registry

1) Assess how closely the software management of change (MOC) process is followed by interviewing relevant Owner/DCO and vendor crew as well as reviewing supporting documentation.
2) Where possible, identify weaknesses and recommend improvements to the process.

2.2 Special Survey

The Special Survey is to include all items listed under the Annual Survey to the satisfaction of the attending Surveyor. Additional attention may be required for new systems placed aboard the asset, for new system automated interfaces, or for new application access methods (remote or mobile) to critical applications or data onboard the asset. The intent of the Special Survey is to look across the asset's history since the previous Special Survey to develop an appreciation for what hardware, software or Company capability changes have occurred that may have invalidated assumptions associated with prior security conditions or risk profiles.

3. Facility Survey

A Company that request for a Facility Survey, shall follow the 5-step process shown in Section 1.C.3, Fig 1.1. Capability assessment process.

The intent of the Facility Survey is to address integrated systems that pass data or control critical functions between Facility and ship (or platform or other examined asset), including the Company's ability to provide capabilities for cyber safety across the Facility, while specifically looking at interface devices, methods and systems. To this end, a Facility under examination requires a Functional Specification Document (FSD) just as a ship or offshore asset requires.

At each Facility Survey, the Surveyor is to perform an integrated software and hardware configuration audit to include verification of the following:

1) Check of asset records against the Facility's Functional Specification Document (FSD) to verify accuracy of asset management efforts.
2) Change control procedures include periodic audits to confirm that procedures are also being followed.

3) Examination of interface control systems in FSD
4) Examination of access control lists and access grant procedures for interface control systems and remote access systems as listed in FSD
5) Examination of Software Registry in FSD
6) Review of all control system Hardware Registry entries
7) Review records of virus and malicious software scans, and perimeter protective device logs of any events of specific interest.
8) Review records of cyber-enabled system incidents and the attendant incident response efforts, including service restoration and post-event analyses.

3.1 Examination of Software Registry

1) Identify all control software that has been changed since the last audit.
2) Record each software item change.
3) Inspect all software hosted on the changed equipment identified in 2.1.1.
4) Record software changes on changed equipment in the Software Registry.
5) Identify all documentation impacted by the changes.
6) Record all changed documentation in the software registry.
7) Note any software changes identified that were not listed on the registry.

3.2 Review of Integrated Control System's Hardware Registry

1) Assess how closely the software Management of Change (MOC) process is followed by interviewing relevant Company/DCO and vendor crew as well as reviewing supporting documentation.
2) Where possible, identify weaknesses and recommend improvements to the process.

3. Modifications, Damage and Repairs

When it is intended to carry out any modifications to the automated and cyber-enabled system that affects the Cybersecurity notation of the vessel or facility, the details of such modifications are to be submitted for approval and the work is to be carried out to the satisfaction of the Surveyor.

When an automated and cyber-enabled system that affects the Cybersecurity notation of the vessel or facility has suffered any damage, which may affect classification, BKI is to be notified and the damage is to be assessed by a Surveyor.

Where an automated and cyber-enabled system suffers a premature or unexpected failure, and are subsequently repaired or replaced without Surveyor attendance, details of the failure, including the damaged parts where practicable, are to be retained onboard for examination by the Surveyor during the next scheduled survey.

If failures are deemed to be a result of inadequate or inappropriate maintenance, the maintenance manual is to be amended and resubmitted for approval.

C. Testing

1. Onboard Testing

While the control system is installed onboard and testing is to be performed, the Company, SBI, and Verification and Validation (V&V) personnel are to agree on the functions or functionality to be tested and the safe method to perform the testing.

Tests or scenarios identified as having risk to safety, environmental, or equipment impacts damage are not to be tested onboard.

The Surveyor is to observe onboard testing and testing results as identified by test plans and scenarios. The Surveyor will not participate in any other role during testing.

2. Safety of personnel

Safety of personnel and equipment are to be considered by the Company and the Surveyor reflected in:

- The cybersecurity assessment and test plans, equipment setup, and other activities at the testing location (at factory or onboard) for safety of personnel and protection of equipment and the environment during execution of the Cybersecurity Assessment.
- The re-activation of the system(s), from testing state to normal, controlling equipment for safety of personnel, equipment, and the environment.